Cisco Wholesale Voice Solution Design and Implementation Guide

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

Customer Order Number:
Text Part Number: OL-1477-01

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

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

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

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

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

Cisco Wholesale Voice Solution Design and Implementation Guide

CONTENTS

Preface

The Cisco Wholesale Voice Solution is a service that provides trunk-level transport of global switched telephone traffic distributed by means of VoIP (voice over IP). The objective of this solution, or set of solutions, is to give service providers essential information about the required architecture design, network components, software features, functional areas, and provisioning methodologies needed to run a VoIP wholesale service.

This preface presents the following major topics:

- Document and Solution Release
- Audience
- Scope
- Document Organization
- Related Documents
- Document Conventions
- Obtaining Documentation
- Obtaining Technical Assistance

Document and Solution Release

This is the first release of this document, which covers Release 2.0(0) of the Cisco Wholesale Voice Solution. Release 1.0 contained a subset of the current features. Software upgrades or bug fixes to Release 2.0 will be indicated by 2.0(1), 2.0(2), and so on. As significant new features are added, the subsequent major releases will be indicated by 3.0(0), 4.0(0), and so on.

Audience

The target audience for this document is assumed to have basic knowledge in the following areas:

- Familiarity with basic UNIX commands and operations, in order to configure the Cisco SC2200 Signaling Controller
- Familiarity with configuring T1/E1 signaling on the Cisco 3600 Series
- Familiarity with configuring ISDN PRI signaling on the Cisco AS5300
- Familiarity with configuring a basic H.323 gateway on the Cisco AS5300

- Familiarity with configuring a basic H.323 gatekeeper on the Cisco AS3600 Series

Scope

This document presents the fundamental design and configuration information that is required to establish the various services provided by the Cisco Wholesale Voice Solution. Service provider networks may have additional requirements that are beyond the scope of this document.

In addition, this document is primarily for Cisco products. To establish and maintain third-party products and applications that may be a part of the Cisco Wholesale Voice Solution, refer to the documentation provided by the vendors of those products.

Document Organization

The major sections of this document are as follows:

Section	Title	Major Topics
Chapter 1	Introduction	Provides basic network diagrams of services provided.
Chapter 2	Provisioning the Gatekeeper Core	Discusses H.323 network and components, dial plans, configuration basics, fault tolerance, security, timing, interconnecting to other service providers, configuring back-to-back gateways, establishing core components.
Chapter 3	Provisioning Shared Support Services	Discusses AAA billing, using NTP, enabling SNMP, using a RADIUS MIB, provisioning OSP servers to the gateway, provisioning services to support audio prompts.
Chapter 4	Provisioning Non-SS7-Based POPs	Discusses provisioning issues related to applications that do not require SS7 signaling.
Chapter 5	Provisioning SS7-Based POPs	Discusses provisioning issues related to the Cisco SC2200 and the Cisco Signaling Link Terminal
Glossary	Glossary	Defines terms used in this document

Related Documents

The majority of the documents referred to in the *Cisco Wholesale Voice Solution Design and Implementation Guide* are available online. They are discussed as you need to refer to them. In the electronic (PDF) version of this document you can click on the URL (Uniform Resource Locator, often referred to as the website) associated with the title of a document, and the selected document will appear within the Adobe Acrobat application window. You can also use the Text Select Tool (third icon from the top, at the left of the Acrobat application window) to copy a URL from the PDF document and paste it into the location field of your browser.

Viewing Online Documents in Your Browser

As you click on links, the files you select may be added to the current document. When you close the file, you will be prompted to save the file. (You will not be able to save the file to a CD.) If you choose not to save the larger file that is created, click *No* when prompted to save the file. However, if you acquire documents that you want to save in a new file, you can save that file to another disk or drive with a new name of your own choosing. Set the following preferences within the Acrobat application to open weblinks in your browser, rather than within Acrobat.

You can obtain the latest version of Adobe Acrobat Reader at http://www.adobe.com.

Step 1 Select the browser you want to use.

- **a.** From the Acrobat main menu, choose File > Preferences > Weblink. The Weblink Preferences window opens.
- **b.** In the Weblink Preferences window, click Browse (or Select) and locate the browser you wish to use.
- **c.** Then select Connection Type from the pull-down menu. Choose Standard if your browser is not listed.
- **d.** Click OK to save your settings.

Step 2 Make sure that Acrobat opens weblinks in your browser.

- **a.** From the Acrobat main menu, choose File > Preferences > Web Capture. The Web Capture Preferences window opens.
- **b.** In the Web Capture Preferences Window, choose Open Weblinks: In Web Browser.
- **c.** Click OK to save your settings.

Document Conventions

Command descriptions use the following conventions:

boldface font	Commands and keywords are in **boldface**.
italic font	Arguments for which you supply values are in *italics*.
[ ]	Elements in square brackets are optional.
{ x | y | z }	Alternate keywords are grouped in braces and separated by vertical bars.
[x | y | z]	Optional alternative keywords are grouped in brackets and separated by vertical bars.
string	A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.

Screen examples use the following conventions:

`screen` font	Terminal sessions and information the system displays are in `screen` font.
`boldface screen` font	Information you must enter is in **`boldface screen`** font.[1]
italic screen font	Arguments for which you supply values are in *italic screen* font.
⟶	This pointer highlights an important line of text in an example.
^	The symbol ^ represents the key labeled Control. For example, the key combination ^D in a screen display means hold down the Control key while you press the D key.
< >	Nonprinting characters, such as passwords, are in angle brackets in contexts where italic font is not available.
[ ]	Default responses to system prompts are in square brackets.
!, #	An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.

[1] As this document makes use of annotated configurations, the rigorous use of boldface type to indicate what the user must enter is relaxed.

Notes use the following conventions:

Note Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the publication.

Timesavers use the following conventions:

Timesaver This symbol means *the described action saves time*. You can save time by performing the action described in the paragraph.

Cautions use the following conventions:

Caution Means *reader be careful*. In this situation, you might do something that could result in equipment damage or loss of data.

Tips use the following conventions:

Tip This symbol means the following information *will help you solve a problem*. Th etips information might not be troubleshooting or even an action, but could be useful information, similar to a Timesaver.

Obtaining Documentation

The following sections provide sources for obtaining documentation from Cisco Systems.

World Wide Web

You can access the most current Cisco documentation on the World Wide Web at the following sites:

- http://www.cisco.com
- http://www-china.cisco.com
- http://www-europe.cisco.com

Documentation CD-ROM

Cisco documentation and additional literature are available in a CD-ROM package, which ships with your product. The Documentation CD-ROM is updated monthly and may be more current than printed documentation. The CD-ROM package is available as a single unit or as an annual subscription.

Ordering Documentation

Cisco documentation is available in the following ways:

- Registered Cisco Direct Customers can order Cisco Product documentation from the Networking Products MarketPlace:

  http://www.cisco.com/cgi-bin/order/order_root.pl
- Registered Cisco.com users can order the Documentation CD-ROM through the online Subscription Store:

  http://www.cisco.com/go/subscription
- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco corporate headquarters (California, USA) at 408 526-7208 or, in North America, by calling 800 553-NETS(6387).

Documentation Feedback

If you are reading Cisco product documentation on the World Wide Web, you can submit technical comments electronically. Click **Feedback** in the toolbar and select **Documentation**. After you complete the form, click **Submit** to send it to Cisco.

You can e-mail your comments to bug-doc@cisco.com.

To submit your comments by mail, use the response card behind the front cover of your document, or write to the following address:

Attn Document Resource Connection
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Obtaining Technical Assistance

Cisco provides Cisco.com as a starting point for all technical assistance. Customers and partners can obtain documentation, troubleshooting tips, and sample configurations from online tools. For Cisco.com registered users, additional troubleshooting tools are available from the TAC website.

Cisco.com

Cisco.com is the foundation of a suite of interactive, networked services that provides immediate, open access to Cisco information and resources at anytime, from anywhere in the world. This highly integrated Internet application is a powerful, easy-to-use tool for doing business with Cisco.

Cisco.com provides a broad range of features and services to help customers and partners streamline business processes and improve productivity. Through Cisco.com, you can find information about Cisco and our networking solutions, services, and programs. In addition, you can resolve technical issues with online technical support, download and test software packages, and order Cisco learning materials and merchandise. Valuable online skill assessment, training, and certification programs are also available.

Customers and partners can self-register on Cisco.com to obtain additional personalized information and services. Registered users can order products, check on the status of an order, access technical support, and view benefits specific to their relationships with Cisco.

To access Cisco.com, go to the following website:

http://www.cisco.com

Technical Assistance Center

The Cisco TAC web site is available to all customers who need technical assistance with a Cisco product or technology that is under warranty or covered by a maintenance contract.

Contacting TAC by Using the Cisco TAC Website

If you have a priority level 3 (P3) or priority level 4 (P4) problem, contact TAC by going to the TAC website:

http://www.cisco.com/tac

P3 and P4 level problems are defined as follows:

- P3—Your network performance is degraded. Network functionality is noticeably impaired, but most business operations continue.
- P4—You need information or assistance on Cisco product capabilities, product installation, or basic product configuration.

In each of the above cases, use the Cisco TAC website to quickly find answers to your questions.

To register for Cisco.com, go to the following website:

http://www.cisco.com/register/

If you cannot resolve your technical issue by using the TAC online resources, Cisco.com registered users can open a case online by using the TAC Case Open tool at the following website:

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

Contacting TAC by Telephone

If you have a priority level 1 (P1) or priority level 2 (P2) problem, contact TAC by telephone and immediately open a case. To obtain a directory of toll-free numbers for your country, go to the following website:

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

P1 and P2 level problems are defined as follows:

- P1—Your production network is down, causing a critical impact to business operations if service is not restored quickly. No workaround is available.
- P2—Your production network is severely degraded, affecting significant aspects of your business operations. No workaround is available.

Introduction

The *Cisco Wholesale Voice Solution Design and Implementation Guide* will help you establish the services introduced in the *Cisco Wholesale Voice Solution Overview*. Links to that and other solution-related documentation are available at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/access/sc/rel7/soln/index.htm

The *Cisco Wholesale Voice Solution Overview* discusses many factors that must be taken into account in designing a wholesale voice network. It is expected that you are familiar with that document, and specifically with the interconnect issues, architectural components, and design templates related to the solution.

This chapter presents the following major topics:

- Establishing Required Components
- Establishing Desired Services
- Network Diagrams

Establishing Required Components

If the hardware and software for your chosen service are not yet established, begin by referring to the following chapters:

- Chapter 2, “Provisioning the Gatekeeper Core”
- Chapter 3, “Provisioning Shared Support Services”
- Chapter 4, “Provisioning Non-SS7-Based POPs”
- Chapter 5, “Provisioning SS7-Based POPs”

Each of these provisioning areas is also discussed in Chapter 2, “Solution Architecture,” of the *Cisco Wholesale Voice Solution Overview*.

Establishing Desired Services

To summarize, the services offered by the Cisco Wholesale Voice Solution are as follows:

- Service A: Minutes Aggregation and Resale (Including ASP Termination)
- Service B: Calling Card Services (Prepaid and Postpaid)

The *Cisco Wholesale Voice Solution Overview* provides templates that cover five interconnect scenarios applicable to these services:

Table 1-1 Templates and Their Descriptions

Template	Description
A1 and B1	TDM-to-TDM Call Topology
A2 and B2	TDM-to-IP Call Topology Using DGK-Based IP Interconnect
A3 and B3	TDM-to-IP-Based Interconnect with OSP
A4 and B4	IP-to-IP-Based Interconnect (Transit Network) with DGK
A5 and B5	IP-to-IP-Based Interconnect (Transit Network) with OSP

The templates discuss design issues or considerations with respect to the following categories: dial plan, billing/settlement, security, and prompting. Both Service A and Service B share the first three categories. However, card services are unique in that they require prompting to interact with the customer. Table 1-2 shows where in this document the above four categories are discussed with respect to provisioning.

Table 1-2 Dial Plan, Billing/Settlement, Security, and Prompting Discussions

Topic	Location
Dial Plan	Dial Plans and Number Normalization, page 2-4
Billing/Settlement	Chapter 3, “Provisioning Shared Support Services”
Security	Providing Security, page 2-34
Prompting	Provisioning Services to Support IVR, page 3-19

In addition, the *Cisco Wholesale Voice Solution Overview* provides templates related to dial plan, billing/settlement, and security for the following service options:

- Limited Egress Carrier-Sensitive Routing
- Interconnect to Clarent-Based Clearinghouses

The implementation of the above options is also discussed later in this design and implementation guide.

Network Diagrams

To assist you in provisioning through an understanding of end-to-end topologies, or provisioning spaces, this section presents a variety of high-level network views that cover the following scenarios:

- Basic Aggregation Model
- Aggregation Model with Card Services (Prepaid and Postpaid)

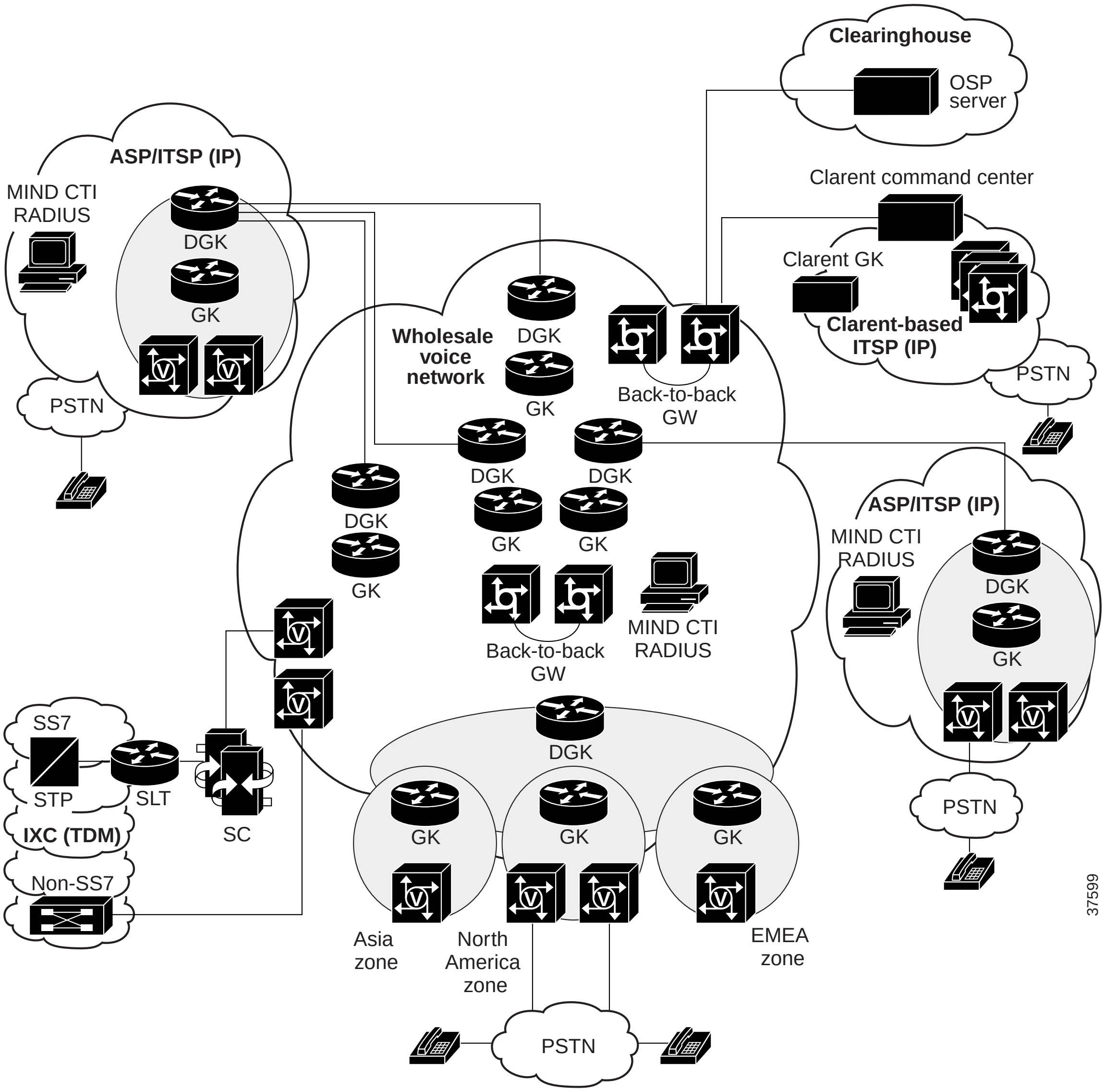
The key sectors of these models will be referred to as various provisioning modules are addressed, with attention to the command-line specifics appropriate to each provisioning sector.

Basic Aggregation Model

Figure 1-1 illustrates the scope of provisioning space for a basic aggregation model that does not use OSP (Open Settlements Protocol) resources. In addition to GKs and DGKs, note especially the following optional components:

- An OSP clearinghouse
- A Clarent Command Center with Clarent GKs
- A MIND CTI RADIUS server
- back-to-back GWs

Figure 1-1 Basic Aggregation Model



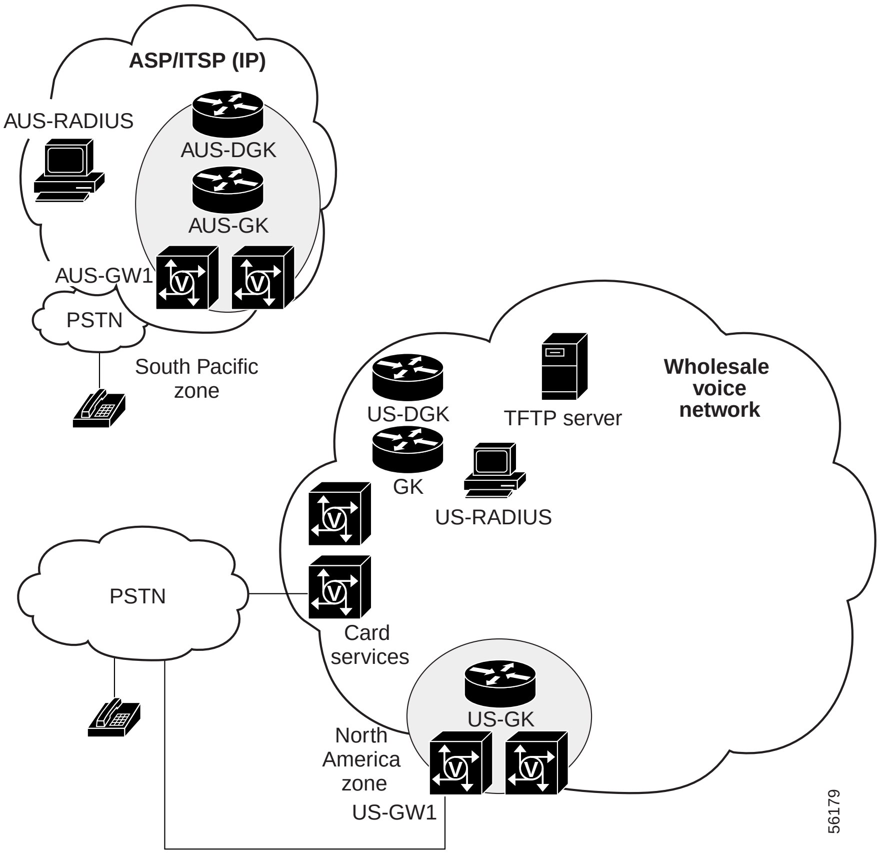
Aggregation Model with Card Services (Prepaid and Postpaid)

Figure 1-2 (a simplified version of the previous two network diagrams) illustrates the scope of provisioning space for an aggregation model that provides both prepaid and postpaid card services. Of concern here are the following:

- A TFTP server, which hosts audio prompt files in addition to storing Cisco IOS image and configuration files
- An AAA/RADIUS billing application server (here called US-RADIUS) in the US zone, which provides the accounting function

Note MIND CTI (http://www.mindcti.com) is a candidate vendor of the accounting application.

Figure 1-2 Aggregation Model for Card Services (Prepaid and Postpaid)



To establish the core components illustrated in these figures, continue with Chapter 2, “Provisioning the Gatekeeper Core.”

CHAPTER 2

Provisioning the Gatekeeper Core

Introduction

This chapter presents the following major topics:

- The Gatekeeper Core and Its Components

  —Discusses the basic components of the gatekeeper core, namely gateways, gatekeepers, and directory gatekeepers

- Understanding Configuration Basics, page 2-8

  —Illustrates how to configure core components in a wholesale VoIP service provider network

- Establishing Core Components, page 2-56

  —Provides links to online references for how to install Cisco hardware

The Gatekeeper Core and Its Components

The infrastructure of a traditional gatekeeper core functional area consists of gateways (GWs) and gatekeepers (GKs). In a typical service provider network, a number of GWs are deployed at POPs throughout the service provider's coverage area. A GK is used to group these GWs into logical zones of control and perform all call routing between the zones.

However, larger H.323 VoIP networks may consist of multiple GKs, which segment the network into numerous local zones. In this case, GKs must communicate with each other in order to route calls between GWs located in different zones. To simplify the administration of dial plans for these multi-GK networks, Cisco introduces the concept of a directory gatekeeper (DGK), which is responsible for routing calls between local GKs.

With respect to the dial plan, each component within the H.323 network is responsible for a portion of the entire VoIP dial plan. GWs are responsible for making *edge* routing decisions between the PSTN and the H.323 network, while GKs and DGKs handle the *core* call routing logic between devices within the H.323 network. The configuration requirements for each of these network components are detailed in this chapter.

For example, when presented with a call, GWs determine whether a call should be sent out to the PSTN or into the H.323 VoIP network. If a call is sent into the H.323 VoIP network, then the GW asks the GK to select the best endpoint to receive the call. From its routing table, the GK may find that this endpoint is a device within its own local zone of control, in which case the GK simply supplies the IP address of the terminating endpoint. Alternatively, it may determine that the endpoint resides under the control of another remote GK. In this case, the GK forwards the location request (LRQ) either to the remote GK directly, or through a DGK. The remote GK ultimately responds with the address of the terminating endpoint. Figure 2-1 shows the relationship of the components that constitute the gatekeeper core, with VoIP-enabled GWs providing access to the PSTN.

Figure 2-1 Components of the Gatekeeper Core

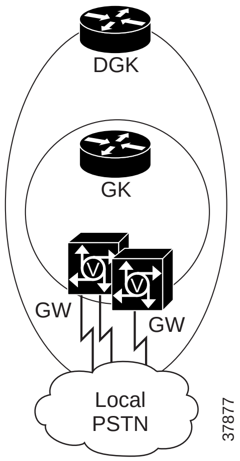


Table 2-1 summarizes the functions of the components of the gatekeeper core.

Table 2-1 Compoents of Gatekeeper Core and Their Functions

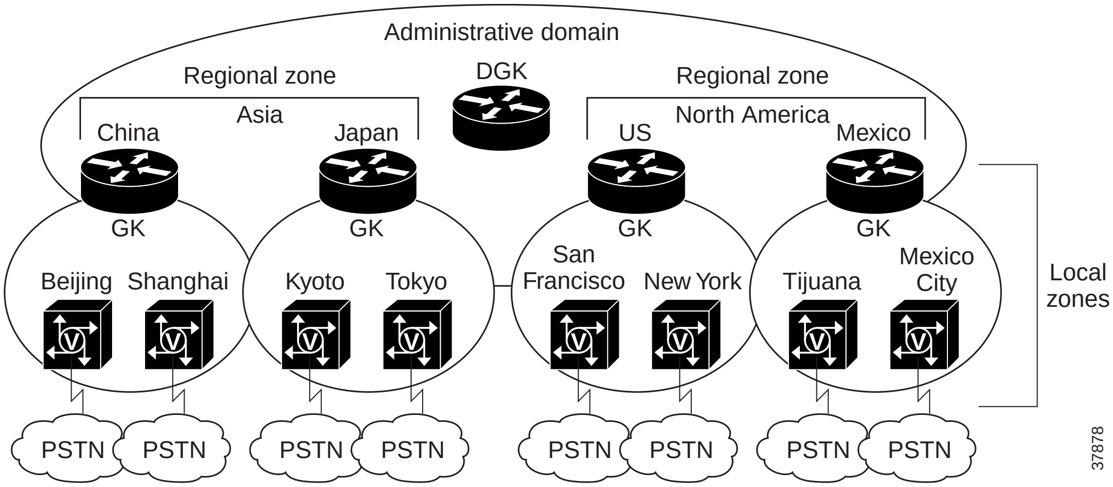
Component	Function
Directory Gatekeeper (DGK)	Performs call routing search at highest level (example: country code)
	Distributes country codes among other DGKs
	Forwards LRQ to partner DGK if call does not terminate in local SP DGK
Gatekeeper (GK)	Performs call routing search at intermediate level (example: NPA-NXX)
	Distributes NPA among other GKs
	Provides GW resource management (examples: RAI, gw-priority)
	Provides zone maintenance
Gateway (GW)	Acts as interface between PSTN and IP network
	Normalizes numbers from PSTN before they enter IP network
	Normalizes numbers from IP network before they enter PSTN
	Contains the dial peer configuration
	Registers to a GK

For an example of these components in a large-scale H.323 VoIP network, see A Large-Scale H.323 VoIP Network, page 2-3.

A Large-Scale H.323 VoIP Network

Figure 2-2 illustrates the relationship of GWs, GKs, and DGKs in a large-scale H.323 VoIP network.

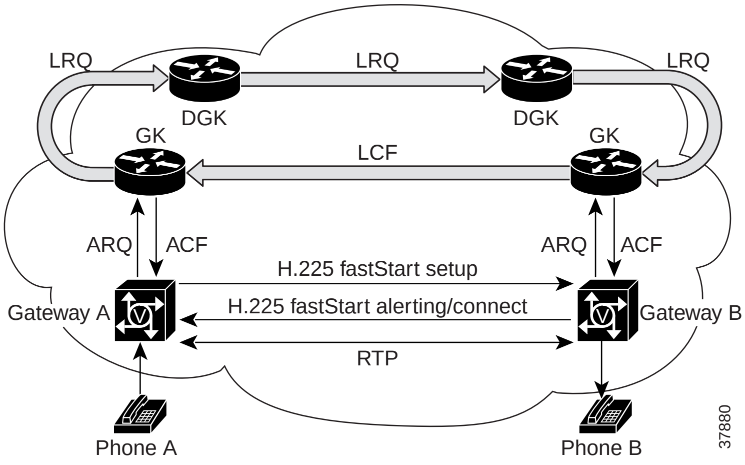
Figure 2-2 Relationship of Gateways, Gatekeepers, and Directory Gatekeepers



The communication between GWs and GKs is based on standard H.323v2 registration, admission, and status (RAS) messages. GWs query GKs for routes by means of RAS admission request/confirm (ARQ/ACF) messages. Cisco GKs and DGKs also communicate with each other by means of RAS location request/confirm (LRQ/LCF) messages. Figure 2-3 illustrates an example RAS message sequence when phone A calls phone B. For additional information about H.323v2 RAS messaging, refer to Cisco H.323 Version 2 Phase 2, at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t1/h323v2p2.htm

Figure 2-3 Example of RAS Messaging when Phone A Calls Phone B



Dial Plans and Number Normalization

This section discusses the basic principles underlying dial plans, which require configuring POTS and VoIP dial peers, and the related number-translation process known as "number normalization."

Overview of the Dial Plan

The dial plan is the method by which individual blocks of telephone numbers (technically, E.164 addresses) are assigned to physical facilities, or circuits. For large-scale service provider networks, dial plans consist of the following:

- A grouping of E.164 prefixes with respect to zones and zone GKs
- An assignment of E.164 address blocks to POPs and POP GWs
- The normalization, prefixing, and digit stripping of telephone numbers (number translation or "normalization") at the POP GWs
- The establishment of POTS and VoIP dial peers at the GWs

POTS dial peers define the phone numbers or prefixes of attached telephony devices, and the VoIP dial peers define the IP address of the remote device (H.323 GW, GK, or endpoint) that is connected to remote phone numbers. POTS dial peers will always point to a voice port on the router, while the destination of a VoIP dial peer will always be the IP address of a device that can terminate the VoIP call.

Distributing the H.323 Dial Plan

Good dial-plan architecture relies on effectively distributing the dial plan logic among the GW and GK components. Isolating H.323 devices to a specific portion of the dial plan reduces the complexity of the configuration, so each component can focus on accomplishing specific tasks. Generally, local POP-specific details are handled at the local GW, whereas higher-level routing decisions are passed along to the GKs and DGKs. A well-designed network consists of keeping the majority of the dial plan logic at the GK and DGK devices.

General Design Methodology

It is important to apply some basic design principles when designing a large-scale service provider dial plan.

1. Keep the design hierarchical.

   Strive to keep the majority of dial plan logic (for routing decisions and failover) at the highest component level. The DGK would generally be considered the "highest" device. With a hierarchical design, the addition and deletion of zones becomes more manageable. For example, the scaling of the overall network is much easier when configuration changes must be made to only a single DGK and a single zone GK—rather than to all the zone GKs.

2. Keep provisioning simple.

   Keep the dial plan on the GWs and GKs as simple and symmetrical as possible. On the GWs, try to keep consistent dial plans, using translation rules to manipulate the local digit dialing patterns. These number patterns can be "normalized" into a standard format or pattern before the digits enter the VoIP core. By putting digits into a standard format, you simplify GK zone prefix provisioning and make GW dial peer management easier.

   This methodology helps to reduce dial peer configurations on the outgoing POTS interface. If the GK can be provisioned to direct only calls of a certain area code to a particular GW, then you would not need to provision all the individual GWs with their respective area codes. Instead you may be able to generalize the GW configurations. By normalizing the number, you also reduce the length of zone prefix searches—and reduce the time to search for a zone prefix match. For example, if you have the digit pattern 0118943xxxx, you can send the number as only 8943xxxx, and have the gatekeeper search on 89 instead of on 01189.

3. Reduce postdial delay.

   Consider the effects of postdial delay in the network. GW/GK zone design, translation rules, and sequential LRQs all can increase postdial delay. Strive to use these tools efficiently in order to reduce postdial delay.

4. Design for availability and fault tolerance.

   Consider overall network availability and call success rate. Using a Cisco alternate gatekeeper, sequential LRQs, and Hot Standby Routing Protocol (HSRP) helps to provide redundancy and fault tolerance in the H.323 network.

Establishing a Dial Plan

Designing a quality dial plan is essential to increasing network efficiency and maintainability. This section introduces a series of topics related to establishing a dial plan:

- POTS and VoIP Dial Peers
- Number Translation or Normalization, page 2-6
- Technology Prefixes, page 2-7
- Prefix Search in DGKs and Local Zones, page 2-8

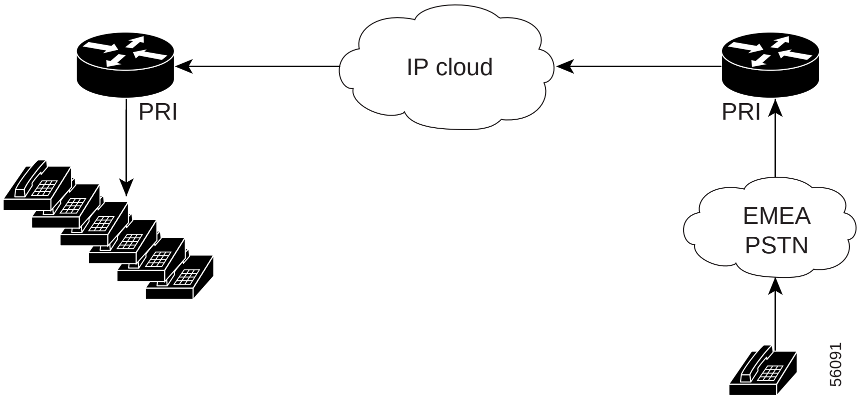
These are discussed below.

POTS and VoIP Dial Peers

Consider two VoIP-enabled access GWs, one originating and one terminating, that transport a PSTN-to-VoIP call through the IP cloud. Figure 2-4, using the example of the EMEA PSTN, illustrates this basic direct inward dial (DID) scenario.

Caution Cisco recommends that you make routing or dialing transparent to the user. For example, where possible avoid secondary dial tones from secondary switches. Enabling **direct-inward-dial** suppresses secondary dial tone, and therefore DID must be enabled when a GW interfaces to a PSTN switch. The switch normally provides dial tone, but does not send dial tone to the GW when DID is enabled. This issue is discussed in *Configuring Voice over IP*, at the following URL:
http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/multi_c/mcprt1/mcdvoip.htm

Figure 2-4 Basic DID Scenario



When DID is used on a POTS dial peer, the number that is dialed (DNIS, the number that accesses the PRI trunk of the GW) automatically becomes the **destination-pattern** number for the IP direction. On the originating GW, there is a POTS dial peer with a destination pattern that matches the DNIS. The dial peer for this example looks like the following:

```
dial-peer voice 100 pots
 direct-inward-dial
 port 0:D
```

The POTS dial-peer (100), which matches the port that the call came in on, has DID configured. The **direct-inward-dial** statement in the dial peer tells the GW to look for a number in a VoIP dial peer that matches the DNIS. It finds it in the following:

```
dial-peer voice 101 voip
 destination-pattern 5710913
 session target ipv4:10.11.253.8    <---terminating GW
```

So a call is made across the IP network to 10.11.253.8 and a match is found in that terminating GW:

```
dial-peer voice 571 pots
 destination-pattern 5710913
 port 0:D
 prefix 5274094
```

This dial peer matches on the dialed number and changes that number to 5274094 with the **prefix** command. The end result is that the user dials one number, gets connected, and never knows that the number reached is totally different from the number dialed.

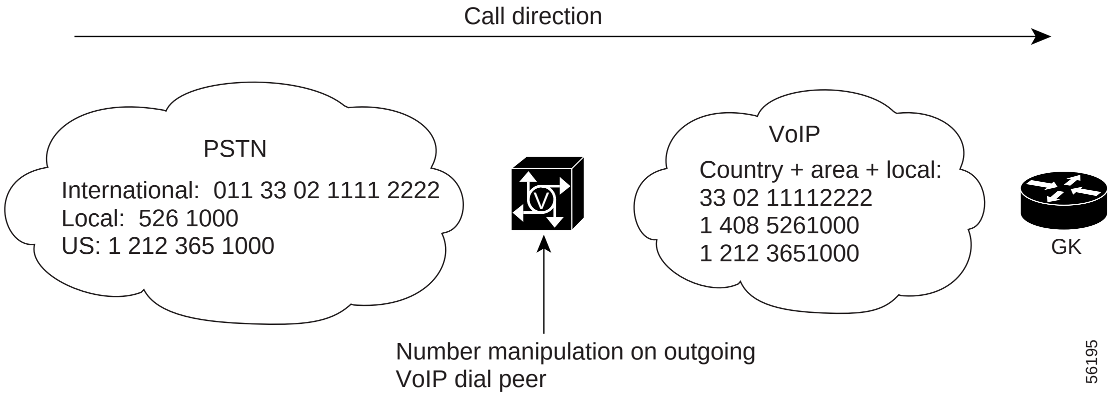
Number Translation or Normalization

GW dial plan configurations are focused on local PSTN access information at the edge of the H.323 network. This includes defining which E.164 prefixes are supported by the PSTN connections of the GW. In large-scale SP-type designs, the GW may also be relied on to perform “digit manipulation,” where the GW takes a calling or called number and strips or adds (prefixes) digits before sending the number to its destination. The process of formatting the calling or called number to a predefined pattern is called “number normalization.”

Figure 2-5 illustrates the process of translating a PSTN number for use in a VoIP network. The GW is connected to the PSTN and VoIP cloud, and uses Cisco IOS translation rules to accomplish digit manipulation. Translation rules can be applied on the GW’s physical port, or in a VoIP dial peer. For example, number manipulation can be configured on the incoming POTS port, the outgoing voip dial peer, or both, to format a 7, 10, 11 or *x*-digit pattern into a fixed 10-digit pattern. The result is a number that has been normalized when it enters the VoIP cloud.

Note Fore more information about translation rules, see *Dial Plan Basics* at the following URL: http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t1/dt0390s7.htm

Figure 2-5 Number Translation from PSTN to VoIP Network



The translation rule above matches digit patterns that begin with [0011-0019] and translates this 4-digit pattern to [1–9], while preserving the remaining digits included in the digit pattern. This effectively strips the 011, a common international access code, and sends the remaining digits to the VoIP GK for call routing.

Translation rules can be used to manipulate both ANI and DNIS numbers. The parameters **destination-pattern**, **answer-address**, **incoming-called-number**, and **numbering-type** can all be configured to match a call’s ANI (Automatic Number Identification) number, that of the originating party, or its DNIS (Dialed Number Identification Service) number, that of the destination party.

Tip To test a translation rule, use the command **test translation rule** <rule number> <number to translate>, as in the following example:

```
US-GW2# test translation-rule 1 011861044445555
4d03h: The replace number  861044445555

US-GW2# test translation-rule 1 00011861044445555
4d03h: number 00011861044445555 can't match any translation rules
```

Note For background and syntax on translation rules, refer to *Dial Peer Enhancements* at the following URL: http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t1/dt0390s7.htm

Technology Prefixes

Also known as a “tech prefix” or a GW’s supported prefix, the technology prefix is an arbitrary, administrator-defined prefix that is used to define a GW type. Analog GWs, which frequently use FXS signaling, do not require the use of a tech prefix, as the E.164 address is registered to the GK. However, digital GWs, which use T1/E1 signaling, require the use of a tech prefix.

For example, you might assign, on an H.320 GW, the prefix 1# to indicate 1-channel calls, and the prefix 2# to indicate 2-channel calls. Alternatively, you might use 1# to indicate voice GWs, 2# to indicate H.320 GWs, 3# to indicate GWs fronting voicemail servers, and so on. So, a call to “1#4085551212” would mean “Use a voice GW to reach 4085551212.”

Each GW must be configured to register its tech prefix with its GK. The user interface varies depending on the vendor, but on Cisco voice GWs it is configured by means of the command **h323-gateway voip tech-prefix**. To facilitate administrative manageability, it is recommended that you use the same tech prefix to represent the same type of GW through all zones in your network.

The caller must prepend the tech prefix to the called number to indicate the type of GW to be used for hopoff. If the call originates through a Cisco voice GW, configuring the matching dial peer with the tech prefix to be prepended does this. If the call originates with an H.323 endpoint, the administrator will have told the user what tech prefix to use for the hopoff GW to the called number.

Caution If a call is not supplied with a tech prefix, you must configure a default tech prefix. Otherwise, the call will fail.

The remote VoIP GWs will still have some dial peers to match digits, but instead of the dial peers pointing to all other VoIP GW, they will use H.323 RAS to register with the GK, and then query the GK for dial plan details. The GK will have all of the zones, zone prefixes, and tech prefixes defined, and will return the information necessary to complete the VoIP call to the originating VoIP GW.

Prefix Search in DGKs and Local Zones

GKs are configured to administer their local country zones and city/area codes (for example, 8610*) to their specific GWs. A DGK is used to handle call routing on the country code alone. Where necessary, GWs can use translation rules to normalize DNIS or ANI numbers before they are propagated to the GK and DGK. For details, see Configuring Translation Rules on the Gateways, page 2-14.

Understanding Configuration Basics

This section discusses the following fundamental activities:

- Building the Gatekeeper Core
- Providing Redundancy for Fault Tolerance
- Providing Redundancy for Software Upgrades
- Configuring Fault Tolerance: Three Methods
- Providing Security
- Providing Network Timing through NTP
- Interconnecting to Other Service Providers
- Configuring Back-to-Back Gateways

Building the Gatekeeper Core

In the following example, a service provider wants to offer voice services with a presence in North America, Asia, and EMEA (Europe, Middle East, and Africa). We will design and configure a GW, GK, and DGK H.323 network that will consist of the following:

- China POP in the Asia zone
- US POP in the North America zone
- France POP in the EMEA zone

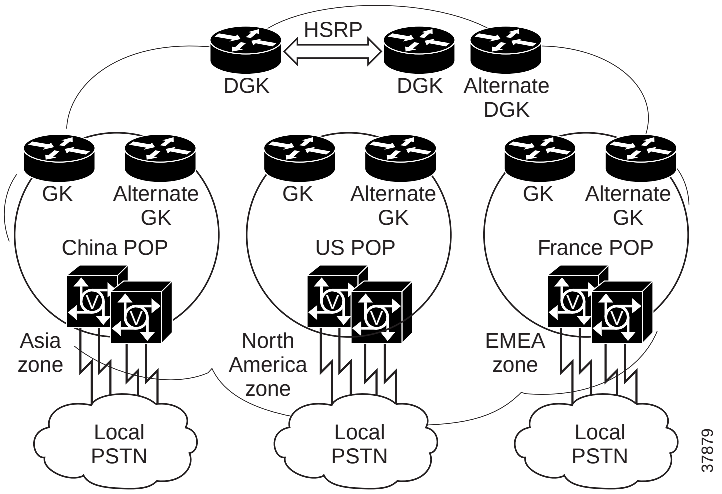
The following are key design goals:

- Ensure successful intracarrier calls between countries.
- Provide management efficiency through a hierarchical GW/GK/DGK relationship.
- Provide number normalization from the PSTN to the VoIP network. This reduces the number of dial peers that must reside at the GW, thus simplifying prefix searches.
- Provide HSRP (Cisco’s Hot Standby Routing Protocol) fault tolerance (continuous service) at the GK and DGK level.

Figure 2-6 is a simplified view of our example wholesale network, whereas Figure 2-7 on page 2-11 shows the detailed topology.

Note See also Figure 1-1 on page 1-3, to review the basic aggregation model and all of its potential components.

Figure 2-6 Example Wholesale Network with Coverage in China, the U.S., and France



Required Steps

Building the core fundamentals consists of the following, as discussed below:

- Building a Zone
- Connecting to Another Zone
- Connecting to Another Administrative Domain
- Additional, but Important, Considerations

Building a Zone

- Configuring Gateways and a Gatekeeper in a Single Zone, with the following subtasks:

  For the GW:

  a. Configuring TDM connections to the PSTN (physical connections and POTS dial peers)

  b. Configuring the GW to register to the GK

  c. Configuring the VoIP dial peers

  d. Configuring number normalization

  For the GK:

  a. Configuring the GK zone name

  b. Configuring the E.164 prefix assignments

  c. Verifying the configuration

Connecting to Another Zone

- Adding a Directory Gatekeeper to the Zones, page 2-22, with the following subtasks:

  a. Configuring the DGK zone name

  b. Configuring the master zone-prefix table

  c. Verifying the configuration

Connecting to Another Administrative Domain

- Interconnecting to a New Administrative Domain, page 2-25

Additional, but Important, Considerations

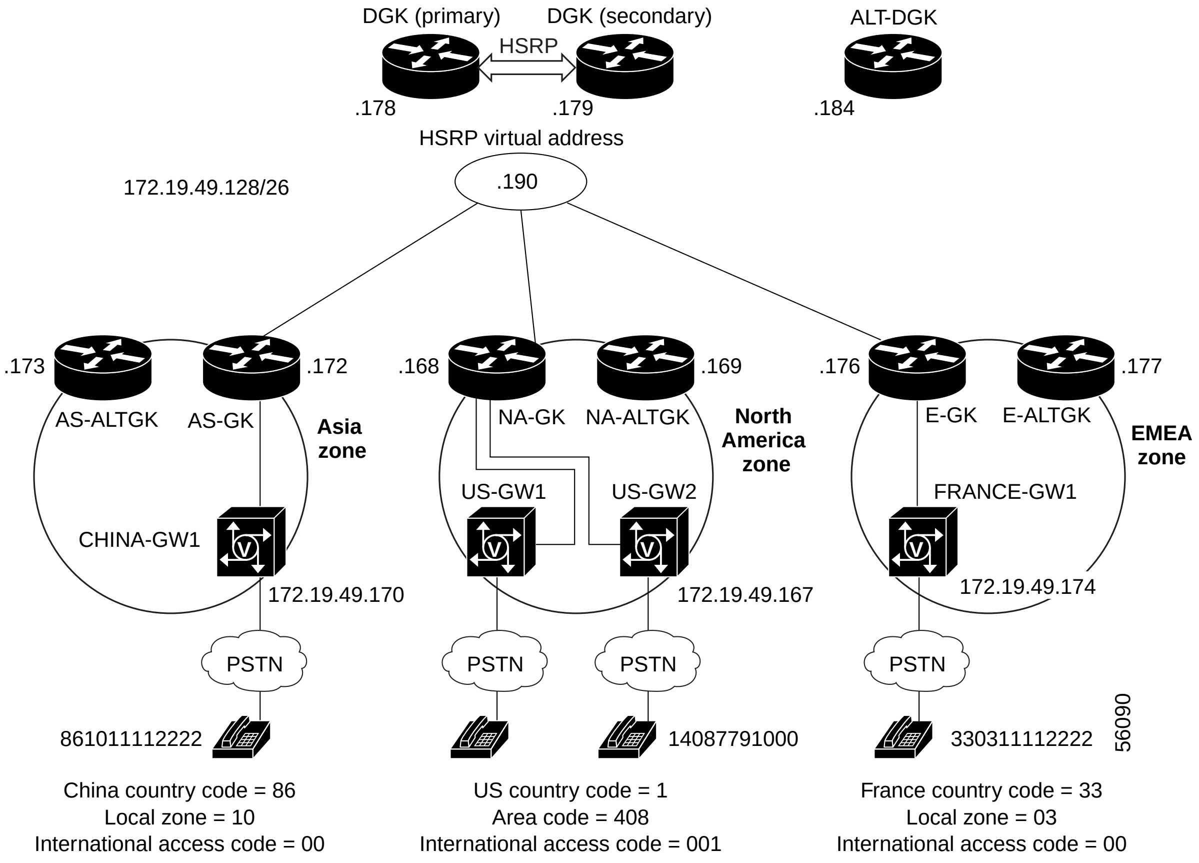
In addition, the following activities are also essential to the proper functioning of the core network.

- Providing Redundancy for Fault Tolerance, page 2-26
- Providing Security, page 2-34
- Providing Network Timing through NTP, page 2-37
- Interconnecting to Other Service Providers, page 2-39

Detailed Network Topology

Figure 2-7 illustrates a detailed topology of our example network. Although it is not illustrated here, calls can originate and terminate on GWs through analog interfaces (FXS, FXO, and E&M), as well as on digital interfaces, such as T1/E1 and PRI.

Figure 2-7 Detailed Network Topology

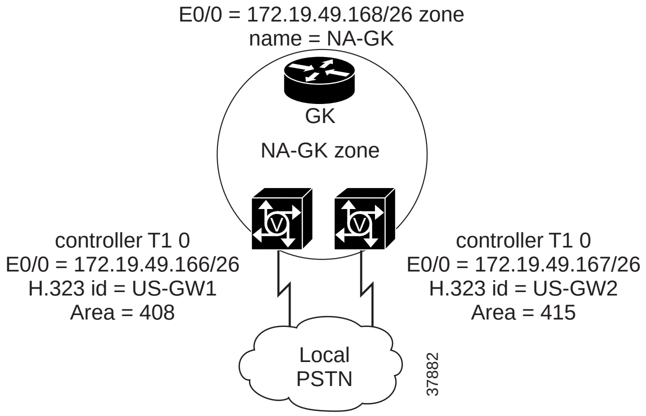


Configuring Gateways and a Gatekeeper in a Single Zone

First we will focus on building a single GK zone. US-GW1 and US-GW2 are GWs in the North American (NA) zone, specifically in the San Francisco POP, and act (collectively) as the GW between the PSTN and the VoIP network. Both GWs register to the zone GK, forming a zone called NA-GK.

Figure 2-8 illustrates the components of zone NA-GK. Figure 2-7 on page 2-11 illustrates the overall network topology.

Figure 2-8 Building a Single GK Zone



Configuring Gateway Interfaces to the PSTN

A look at the configuration file for the two GWs, US-GW1 and US-GW2, illustrates the establishment of T1 facilities. The establishment of E1 facilities is similar. We begin with US-GW1, then proceed to US-GW2. In this example we use Cisco AS5300 GWs.

Note For detailed information about T1 and E1 provisioning, refer to the following URLs:

- Configuring ISDN PRI and Other Signaling on E1 and T1 Lines, at

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/dialts_c/dtsprt3/dcdchant.htm

- Channelized E1 and Channelized T1 Setup Commands, at

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/12cgcr/dial_r/drprt1/drchant.htm

- Configuring Channelized E1 and Channelized T1, at

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/12cgcr/dial_c/dcchant.htm

- E1 R2 Signaling for the Cisco AS5300 and Cisco AS5200 Access Servers, at

http://www.cisco.com/univercd/cc/td/doc/product/access/acs_serv/5300/sw_conf/ios_121/5300r2.htm

Step 1 Do the following on US-GW1.

a. Establish T1 PRI signaling parameters for US-GW1. In this example, framing is ESF, linecode is B8ZS, and timing is being provided by the GW itself. The parameter **pri-group** allocates 24 DS0 channels.

```
controller T1 0
 framing esf
 clock source line primary
 linecode b8zs
 pri-group timeslots 1-24
```

b. Establish the physical interface that the PRI facility from US-GW1 will use. The **0** in **Serial0:23** creates a relationship with the PRI facility that **controller t1 0** established above. **23** indicates that channels 0 through 23 are used. Here the switch type is defined.

```
interface Serial0:23
 no ip address
 isdn switch-type primary-ni
 isdn incoming-voice modem
 no cdp enable
```

c. Establish the voice ports for US-GW1. In this case, the signaling is PRI, and the D-channels must be defined. In this case, we have configured only the first T1 interface for D-channel signaling. The remaining three voice ports are the default settings.

```
voice-port 0:D
!
voice-port 1:1
!
voice-port 2:2
!
voice-port 3:3
!
```

Step 2 Do the following on US-GW2.

a. Establish T1 CAS signaling parameters for US-GW2. Parameters are as for US-GW1. **ds0-group 0** establishes a relationship between a T1 port and 24 DS0 channels (comprising a full T1). In this example, signaling has been defined as E&M, Feature Group B, multifunction tone, with the DNIS option (for DID). The **ds0 busyout** statement places all 24 time slots in the busyout state when they change state.

```
controller T1 0
 framing esf
 clock source line primary
 linecode b8zs
 ds0-group 0 timeslots 1-24 type e&m-fgb mf dnis
 ds0 busyout 24
```

b. Establish the physical interface that the T1 CAS facility from US-GW2 will use. See Step 1a above.

```
interface Serial0:23
 no ip address
 isdn switch-type primary-ni
 isdn incoming-voice modem
 no cdp enable
```

c. Establish the voice ports for US-GW2. See Step 5. Because this GW uses CAS signaling, no D-channel is defined. Again, the remaining three voice ports are the default settings.

```
voice-port 0:0
!
voice-port 1:1
!
voice-port 2:2
!
voice-port 3:3
```

This concludes the basic establishment of facilities and dial peers. To have the GWs register with the GK, as well as to establish dial plans and translation rules, continue with the steps below, with US-GW1 as an example. See also Establishing a Dial Plan, page 2-5.

Configuring the GWs to Register with the GK

We begin with US-GW1, then proceed to US-GW2.

Step 1 Do the following on US-GW1.

a. Establish the interface.

```
interface Ethernet0/0
```

b. Assign an IP address to the interface.

```
ip address 172.19.49.166 255.255.255.192
```

c. Enable H.232 functionality on this interface.

```
 h323-gateway voip interface
```

Caution The above must be the first H.323 command you configure. If you do not do this, the other H.323 commands will not appear following a **show run**.

d. Establish the identity of the GK to which the GW will register. NA-GK is the name of the GK zone, and 1719 is the well-known port for H.323 RAS registration.

```
h323-gateway voip id NA-GK ipaddr 172.19.49.168 1719
```

e. Configure the GW's H.323 ID as US-GW1.

```
h323-gateway voip h323-id US-GW1
```

f. Assign the tech prefix "1#" to the GW when it registers to the GK.

```
h323-gateway voip tech-prefix 1#
```

Note For information about tech prefixes, see Technology Prefixes, page 2-7.

Step 2 On US-GW2, change the IP address and name of the GW and repeat Steps a through f, above.

Configuring Translation Rules on the Gateways

Now we configure the appropriate translation rules on both GWs. The rules will be the same on both GWs. Refer to Number Translation or Normalization, page 2-6. Table 2-2 summarizes the current dialing patterns for each of the GWs in our configuration example. The objective is to use number normalization to reduce the number of dial peers on each GW.

Note For detailed information about translation rules, see Dial Peer Enhancements at the following URL: http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121limit/121x/121xm/121xm_5/ftdpeer.htm

Table 2-2 Dialing Patterns, Codes, and Habits for Detailed Network Topology

Zone	GW	POP	Dialing Pattern	Code	Dialing Habit	Normalized Pattern
North America	US-GW1	US	1.408.527.1000	*Country*: 1 *Area*: 408 *Int'l access*: 011	*Local*: In 408 area code, use 7-digit dialing *Long distance*: Use 1 + area code + local number *International*: outside North America, use 011 (access code) + country code + local city code + local number	country code + city code + local number
	US-GW2	US	1.408.779.1000			
Asia	CHINA-GW1	China POP	861011112222	*Country*: 86 *City*: 010 *Int'l access*: 00	*Local*: In 010 city code, use 8-digit dialing, beginning with 1–9 *Long distance*: Within China, use area code (dialed with 0*x* or 0*xx*) + local number *International*: Outside North America, use 00 (access code) + country code + local city code + local number	
EMEA	FRANCE-GW1	France POP	330311112222	*Country*: 33 *City*: 03 *Int'l access*: 00	*Local*: In 03 area code, use area code (0*x*) + 8-digit local number *Long distance*: Within France, use area code (0*x*) + 8-digit local number *International*: Outside North America, use 00 (access code) + country code + local city code + local number	

Tip The translation rules should be configured to match the local dialing habits within the country in which the GW resides. (The "country code" is also known as the "international calling code.") Match the translation rule with the appropriate outgoing **voip dial-peer**.

Do the following on both US-GW1 and US-GW2.

Step 1 Write a translation rule that strips the international access code, which in this case is 011. This rule is ***translation rule 1***, which applies to the VoIP dial peer.

```
translation-rule 1
 Rule 0 ^0111.% 1
 Rule 1 ^0112.% 2
 Rule 2 ^0113.% 3
 Rule 3 ^0114.% 4
 Rule 4 ^0115.% 5
 Rule 5 ^0116.% 6
 Rule 6 ^0117.% 7
 Rule 7 ^0118.% 8
 Rule 8 ^0119.% 9
```

Step 2 Write a translation rule that adds the North America country code and local area code to the DNIS number. This is ***translation rule 2***, which applies to the POTS dial peer.

```
translation-rule 2
 Rule 0 ^2...... 14082
 Rule 1 ^3...... 14083
 Rule 2 ^4...... 14084
 Rule 3 ^5...... 14085
 Rule 4 ^6...... 14086
 Rule 5 ^7...... 14087
 Rule 6 ^8...... 14088
 Rule 7 ^9...... 14089
```

Configuring Dial Peers on the Gateways

As the VoIP dial peers are the same on both GWs, do the following on both US-GW1 and US-GW2. However, different POTS dial peers are needed, to serve different area codes.

Step 1 Configure the VoIP dial peers on both GWs. Refer to the discussion in POTS and VoIP Dial Peers, page 2-5.

a. Configure a VoIP dial peer for an international call that requires a country access code (here 011). See the note below for a discussion of the variable parameter ***T***.

```
dial-peer voice 1 voip
 destination-pattern 011T
 translate-outgoing called 1 <----applies translation rule 1 to dial peer
 session target ras
```

b. Configure a VoIP dial peer for a local 7-digit number. The last two lines, respectively, invoke *translation rule 1* on a match, and cause a RAS ARQ message to be sent to the GK.

```
dial-peer voice 4 voip
 destination-pattern [2-9]......
 translate-outgoing called 2 <----applies translation rule 2 to dial peer
 session target ras
```

c. Configure a VoIP dial peer for an intra-country (in our example, U.S. domestic) call (1-*xxx*-*xxx*-*xxxx*).

```
dial-peer voice 2 voip
 destination-pattern 1T
 session target ras
```

Step 2 Configure POTS dial peers on the GWs. These will vary by area code.

a. Configure a POTS dial peer on US-GW1 for FXS (DID) calls.

```
voice-port 0:D
timeouts interdigit 3
```

Note **timeouts interdigit** <*seconds*> is the interval allowed between each dialed digit (**. . . .**). This interval is also represented by *T* in the country access code above (**destination-pattern 011T**), to allow for a sufficient pause.

```
voice-port 0:D <---assigns voice port 0:D to the dial peer
!
!
!
dial-peer voice 1408 pots
 destination-pattern 1408.......
no digit-strip <----forces matched digits in destination pattern not to be stripped
```

Note The default setting strips matched digits.

```
direct-inward-dial <----recognizes the DNIS number from the PSTN
port 0:D
!
gateway
```

b. Configure a POTS dial peer on US-GW2, noting the different area code. Refer to the step above.

```
voice-port 0:D
!
!
!
dial-peer voice 1415 pots
destination-pattern 1415.......
no digit strip
!
!
direct-inward-dial
port 0:D
!
gateway
```

Summary of a Gateway Configuration

Now look at key elements of the configuration for US-GW2.

```
Current configuration:
!
version 12.1
!
hostname US-GW2
!
!
!
translation-rule 1
 Rule 0 ^0111.% 1
 Rule 1 ^0112.% 2
 Rule 2 ^0113.% 3
 Rule 3 ^0114.% 4
 Rule 4 ^0115.% 5
 Rule 5 ^0116.% 6
 Rule 6 ^0117.% 7
 Rule 7 ^0118.% 8
 Rule 8 ^0119.% 9
```

```
!
translation-rule 4
 Rule 0 ^2...... 14082
 Rule 1 ^3...... 14083
 Rule 2 ^4...... 14084
 Rule 3 ^5...... 14085
 Rule 4 ^6...... 14086
 Rule 5 ^7...... 14087
 Rule 6 ^8...... 14088
 Rule 7 ^9...... 14089
!
!
!
interface Ethernet0/0
 ip address 172.19.49.167 255.255.255.192
 h323-gateway voip interface
 h323-gateway voip id NA-GK ipaddr 172.19.49.168 1719 priority 1
 h323-gateway voip id NA-ALTGK ipaddr 172.19.49.169 1719 priority 2
 h323-gateway voip h323-id US-GW2
!
ip classless
ip route 0.0.0.0 0.0.0.0 172.19.49.129
no ip http server
!
!
voice-port 0:D
!
voice-port 0:D
!
dial-peer cor custom
!
!
!
dial-peer voice 1 voip
 destination-pattern 011T
 translate-outgoing called 1
 session target ras
!
dial-peer voice 2 voip
 destination-pattern 1T
 session target ras
!
dial-peer voice 1415 pots
 destination-pattern 1415.......
 port 0:D
!
dial-peer voice 4 voip
 destination-pattern [2-9]......
 translate-outgoing called 4
 session target ras
!
gateway
!
```

Configuring the Gatekeeper

Follow the steps below to configure the GK. See Building a Single GK Zone, page 2-12.

Step 1 Establish the GK hostname and IP address.

```
hostname NA-GK
!
interface Ethernet0/0
ip address 172.19.49.168 255.255.255.192
!
```

Step 2 Configure the router to be a GK and create a zone prefix table.

a. Establish the identity of the router as a GK.

```
gatekeeper
```

b. Establish a zone name (NA-GK), a domain (netman.com), and an IP address.

```
zone local NA-GK netman.com 172.19.49.168
```

c. Create a zone prefix table for the zone served by US-GW1. This defines NA-GK as the zone for administering the 1408* prefixes. (1408* numbers reside in the GWs belonging to the NA-GK zone.)

```
zone prefix NA-GK 1408* gw-priority 10 US-GW1
```

d. Do the same as in the preceding step, except for the zone served by US-GW2.

```
zone prefix NA-GK 1415* gw-priority 10 US-GW2
```

e. Assign a default technology prefix. (Optional. See Technology Prefixes, page 2-7.)

```
gw-type-prefix 1#* default-technology
```

f. Allow LRQs to be forwarded to other GKs.

```
lrq forward-queries
```

g. Activate the interface.

```
no shutdown
```

Step 3 Verify that the GWs register to the GK.

```
sh gate end
```

When the registration is successful, something like the following appears. The GWs appear as endpoints. The other parameters are self-explanatory.

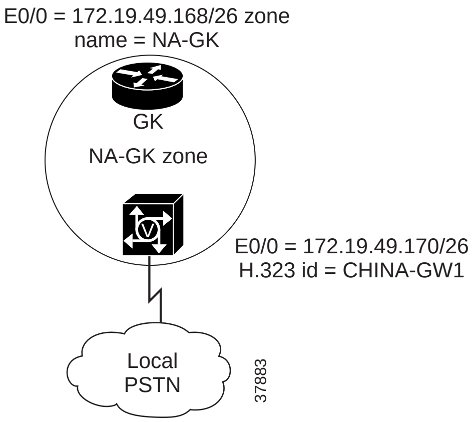
```
GATEKEEPER ENDPOINT REGISTRATION
                    ================================
CallSignalAddr  Port  RASSignalAddr   Port  Zone Name         Type    F
--------------- ----- --------------- ----- ---------         ----    --
172.19.49.166   1720  172.19.49.166   54715 NA-GK             VOIP-GW
    H323-ID: US-GW1
172.19.49.167   1720  172.19.49.167   56615 NA-GK             VOIP-GW
    H323-ID: US-GW2
Total number of active registrations = 2
```

Note Endpoint registration is checked only on the initial RRQ. It is not checked on keep-alive RRQs.

Step 4 Now build a new zone. Refer to Figure 2-9.

We will configure a second zone, AS-GK, located in China. For simplicity, this will consist of one GW at the China POP, and an associated zone GK.

Figure 2-9 Building a New GK Zone



Reviewing the Configurations

The following are example abbreviated configuration files for the gateway CHINA-GW1 and the gatekeeper AS-GK.

Step 1 First look at the GW, noting the following essentials.

```
CHINA-GW1# sh run
Building configuration...

!
hostname CHINA-GW1
!
!
!
translation-rule 2
 Rule 0 ^01.% 8601
 Rule 1 ^02.% 8602
 Rule 2 ^03.% 8603
 Rule 3 ^04.% 8604
 Rule 4 ^05.% 8605
 Rule 5 ^06.% 8606
 Rule 6 ^07.% 8607
 Rule 7 ^08.% 8608
 Rule 8 ^09.% 8609
!
translation-rule 1
 Rule 0 ^0011.% 1
 Rule 1 ^0012.% 2
 Rule 2 ^0013.% 3
 Rule 3 ^0014.% 4
 Rule 4 ^0015.% 5
 Rule 5 ^0016.% 6
 Rule 6 ^0017.% 7
 Rule 7 ^0018.% 8
 Rule 8 ^0019.% 9
!
!
!
interface Ethernet0/0
 ip address 172.19.49.170 255.255.255.192
 h323-gateway voip interface
 h323-gateway voip id AS-GK ipaddr 172.19.49.172 1719
 h323-gateway voip h323-id CHINA-GW1
 h323-gateway voip tech-prefix 1#
!
interface Ethernet0/1
 no ip address
 shutdown
!
ip classless
ip route 0.0.0.0 0.0.0.0 172.19.49.129
no ip http server
!

voice-port 0:D
 timeouts interdigit 3
!
voice-port 0:D
!
!
!
dial-peer voice 8610 pots
 destination-pattern 861011112222
 port 1/0/0
!
dial-peer voice 1 voip
 destination-pattern 001T
 translate-outgoing called 1
 session target ras
!
dial-peer voice 2 voip
 destination-pattern 86T
 session target ras
!
dial-peer voice 3 voip
 destination-pattern 0[1-9]T
 translate-outgoing called 2
 session target ras
!
gateway
```

Step 2 Now look at the GK.

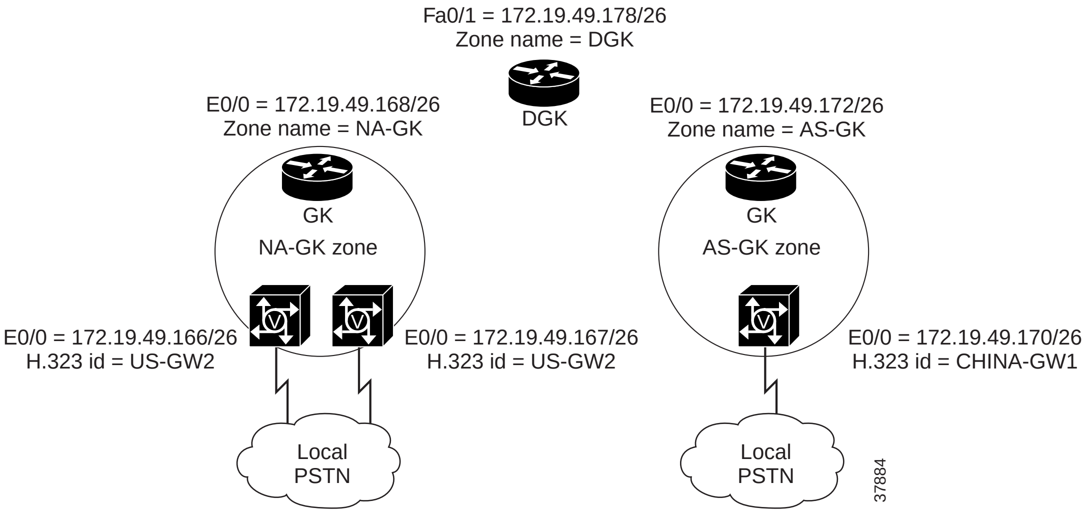
```
AS-GK#sh run
Building configuration...

Current configuration:
!
version 12.1
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname AS-GK
!
enable password pme123
!
!
```

```
!
interface Ethernet0/0
 ip address 172.19.49.172 255.255.255.192
!
interface Ethernet0/1
 no ip address
 shutdown
!
ip classless
ip route 0.0.0.0 0.0.0.0 172.19.49.129
no ip http server
!
!
!
gatekeeper
 zone local AS-GK netman.com 172.19.49.172
 zone remote DGK netman.com 172.19.49.190 1719
 zone remote ALTDGK netman.com 172.19.49.180 1719
 zone prefix AS-GK 8610* gw-priority 10 CHINA-GW1
 zone prefix DGK *
 zone prefix ALTDGK *
 no shutdown
```

Adding a Directory Gatekeeper to the Zones

The following steps add a DGK to the zones that have been established. The directory gatekeeper named DGK will be added to the network to provide call routing between the zone GKs. This DGK will contain the master zone prefix table, relieving the individual GKs of having to maintain the most current information. Figure 2-10 illustrates the relationship of DGK to zones NA-GK and AS-GK.

Figure 2-10 Adding a DGK for Zones NA-GK and AS-GK



Note Consider the following performance relationship between the DGK and the GKs it supports. On the average, the DGK requires one-quarter of the CPU processing capacity needed by the local zone GKs. So if the CPU load on the GK is 40%, then you only need 10% CPU allocation on the DGK. Cisco IOS software has a limit of 5 recursive LRQs; an LRQ is limited to 5 hops. Local zones and LRQ forwarding zones can be mixed.

Follow the steps below to add a DGK.

Step 1 Add the DGK, assigning a name, interface, and IP address (in our example, "DGK" and FastEthernet 0/0 172.19.49.178 255.255.255.192). Refer to Figure 2-10.

```
hostname DGK
!
!
interface FastEthernet0/0
ip address 172.19.49.178 255.255.255.192
duplex auto
speed auto
!
```

Step 2 Configure the zone prefix table on the DGK. A local zone called DGK is established, and the remote zones NA-GK and AS-GK are configured. DNIS numbers that begin with 1 (the NA-GK country code) are handled by NA-GK. DNIS numbers that begin with 86 (the AS-GK country code) are handled by AS-GK. The appropriate zone prefixes are configured to forward LRQs to the respective GKs, as shown below. Again, 1719 is the well-known port for H.323 RAS registration (the GK UDP registration and status port).

```
gatekeeper
zone local DGK netman.com 172.19.49.190
zone remote NA-GK netman.com 172.19.49.168 1719
zone remote AS-GK netman.com 172.19.49.172 1719
zone prefix NA-GK 1*
lrq forward-queries
no shutdown
!
!
line con 0
 transport input none
line aux 0
line vty 0 4
 password pme123
 login
!
end
```

Note Because the DGK sits above the zone GKs, the DGK does not maintain the registration of GWs.

Using Traffic Management Features

If one or more GWs become unduly burdened by incoming calls, there are various ways to manage traffic. This section discusses two techniques:

- Resource Availability Indicator
- Call Admission Control

Resource Availability Indicator

Problems can arise when traffic load causes GWs to reach their capacity. The Resource Availability Indicator (RAI) is an H.323 feature that informs the GK when no circuits (DS0s) or DSPs are available. RAI messages indicate both the availability and unavailability of a GW, depending on the threshold for each that the user can set. RAIs let the GK select the best available GW at the outset, increasing call-completion rates and lowering postdial delay. After the GK receives an RAI from an overburdened GW, it will not assign calls to that GW.

There are two load thresholds: A high value determines when the GW sends the GK an "unavailable" RAI, and the low value determines when the GW sends the GK an "available" RAI. The syntax is as follows:

```
resource threshold [all] [high %-value] [low %-value]
```

Note The default values are 90 for both high and low.

So, to set a high threshold of 90 and a low threshold of 80, we enter the following:

```
gw1(config-gateway)# resource threshold high 90 low 80
```

To see the results, issue the command **show gateway**, as follows.

```
gw1# show gateway

Gateway gw1 is registered to Gatekeeper gk.mwest

H323 resource thresholding is Enabled and Active
H323 resource threshold values"
 DSP: Low threshold 80, High threshold 90
 DS0: Low threshold 80, High threshold 90
```

If only a single GW is within a zone, the GK will give that GW the call, in the hope that there are enough resources to terminate the call. Otherwise, the preferences will reroute the call at the ingress GW.

Call Admission Control

Call admission control (CAC) is another way to assign priority to GWs. The priority of the GW is configured on the GK to prioritize selection from among multiple GWs. The GK can select the most available GW at the outset, to increase call completion rates and lower postdial delay. The usage is as follows:

```
GK(config)# gatekeeper
 GK(config-gk)# zone local west-gk cisco.com 10.1.1.1
 GK(config-gk)# zone prefix west-gk  415666.... gw-pri 10 gw1
 GK(config-gk)# zone prefix west-gk  415777.... gw-pri 10 gw2
```

Note The default priority is 5.

The result is a master list, which you can see with **show gatekeeper**:

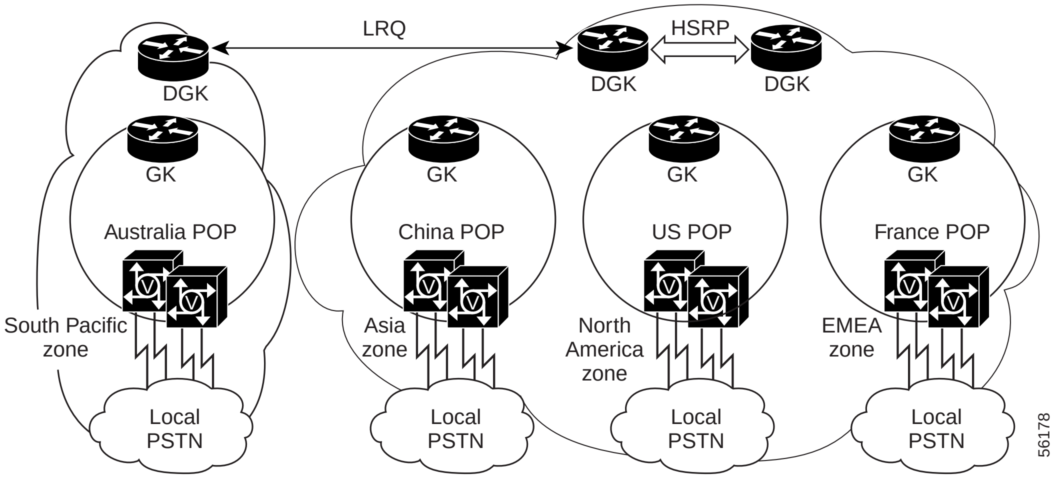
```
master list: gw1, gw2
408666 list: pri 10 gw1; pri 5 gw2
408777 list: pri 10 gw2; pri 5 gw1
```

Interconnecting to a New Administrative Domain

This section discusses how to interconnect to an new administrative domain, such as a new wholesale VoIP provider. The interconnection is between two DGKs, and the DGK of the new SP forwards LRQs to the previously established domain, and vice versa.

Figure 2-11 illustrates the addition of a DGK, AUS-DGK, and the South Pacific zone it maintains. The GK is AUS-GK. The POP is Australia POP, and the country code is 61. The new DGK sends LRQs to the virtual address of the paired DGKs to the right. For information about virtual addresses and enabling redundancy, see Providing Redundancy for Fault Tolerance, page 2-26.

Figure 2-11 Adding a DGK and the South Pacific Zone



The following is an abbreviated configuration that highlights the essentials of configuring a GW in the new DGK zone. Our new GW is AUS-GW1. For details, see Adding a Directory Gatekeeper to the Zones, page 2-22.

```
AUS-GW1#sh run
Building configuration...

Current configuration:
!
!
!
hostname AUS-GW1
!
interface Ethernet0/0
ip address 172.19.49.183 255.255.255.192<----the address of our new GW, AUS-GW1
!
```

```
interface Ethernet0/1
no ip address
shutdown
!
ip classless
ip route 0.0.0.0 0.0.0.0 172.19.49.129
no ip http server
!
!
gatekeeper  <----the following lines are for AUS-GK
zone local NK-AUS-GK newkid.com 172.19.49.183
zone remote NK-DGK newkid.com 172.19.49.185 1719
zone prefix NK-AUS-GK 617* gw-priority 10 NK-AUS-GW1
zone prefix NK-DGK *
no shutdown

<---snip--->

gatekeeper    <----the following lines are for AUS-DGK
zone local NK-DGK newkid.com 172.19.49.185
zone remote NK-AUS-GK newkid.com 172.19.49.183 1719
zone remote DGK netman.com 172.19.49.190 1719
zone prefix NK-AUS-GK 617*
zone prefix DGK *  <---- the route to “DGK” (maintained by the other SP)
lrq forward-queries
no shutdown
```

Note The zone prefix “DGK *,” above, represents zone prefix DGK 1 *, DGK 33 *, and DGK 86 *. See Table 2-4 on page 2-59.

Providing Redundancy for Fault Tolerance

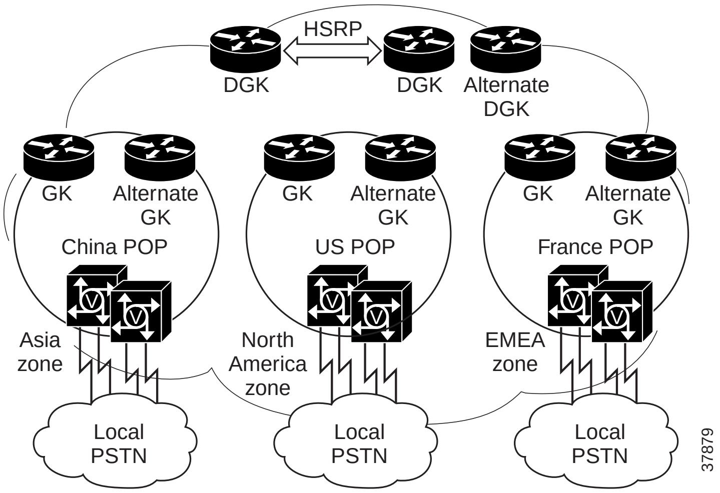
There are three principle methods of providing fault tolerance in large H.323 networks:

- Using Alternate Gatekeepers for Fault Tolerance, page 2-27
- Using HSRP on Directory Gatekeepers, page 2-29
- Using an Alternate Directory Gatekeeper for Fault Tolerance, page 2-30

Figure 2-12 (the same as Figure 2-6 on page 2-9) illustrates a network that provides fault tolerance through HSRP at the DGK level, alternate GKs, and alternate DGKs.

In addition, redundant components contribute considerably in minimizing downtime during software upgrades. For a discussion of things to consider when upgrading Cisco IOS software and other software, see Providing Redundancy for Software Upgrades, page 2-30.

Figure 2-12 Providing Fault Tolerance through Redundancy



Fault tolerance and redundancy within H.323 networks is most important at the DGK level. Current and future versions of Cisco IOS allow DGK redundancy to be configured for alternate DGKs, and Cisco's HSRP (Hot Standby Routing Protocol) to be configured for DGKs.

Caution Although both approaches can be used, Cisco recommends that only HSRP be used on DGKs, and that alternate GKs be used for zone GKs.

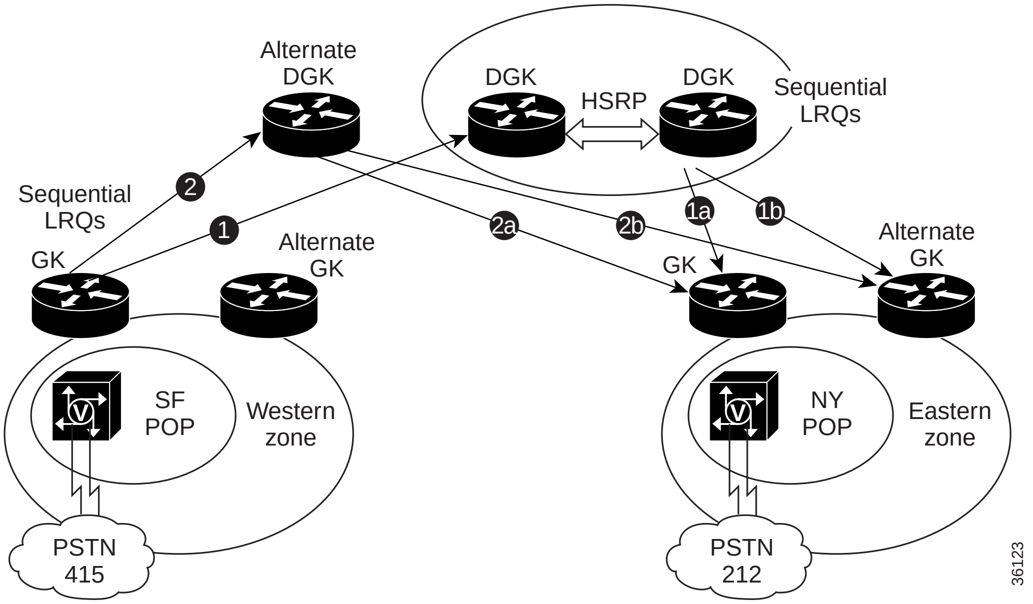
Using Alternate Gatekeepers for Fault Tolerance

In an alternative to the HSRP approach, using an alternate GK at the zone level provides redundancy. This enhancement allows a GW to use up to two alternate GKs as a backup in case a primary GK fails. More specifically, the GWs are configured to register to a primary and an alternate GK. If the primary GK fails, the alternate GK can then be used for call routing, and maintain call routing without call failure. Because Cisco GKs do not communicate registration states between each other, sequential LRQs must be configured on the GKs and DGKs to accommodate zone fragmentation. The configuration of the GKs is similar to that of the DGKs discussed in Method 3: Configuring an Alternate DGK, page 2-33.

Note Cisco IOS release 12.1(2)T introduced sequential LRQs, whereby LRQs are transmitted sequentially —instead of in a unicast blast of LRQs. This is a significant advantage over HSRP, because backup GKs no longer must be colocated in the same geographical location.

Figure 2-13 illustrates a fault-tolerant architecture in an example network that uses alternate GKs.

Figure 2-13 Fault-Tolerant Architecture using Alternate GKs



GWs may be configured to register to a primary GK and an alternate GK if the primary GK fails. This implies that at any given time, a GW may be registered to either its primary or alternate GK. Since Cisco GKs do not communicate registration states between each other, sequential LRQs must be configured on the GKs and DGKs to accommodate zone fragmentation.

For example, a GK in the Western zone supports GWs in San Jose (408) and San Francisco (415). Under normal circumstances, when San Jose calls San Francisco, the route is resolved in the local primary GK. However, assume that San Jose fails over to the alternate GK while San Francisco remains on the primary GK. To continue to support regional call completion within the Western zone, the primary and alternate GKs must be provisioned to send local prefixes to each other if no local resources exist (for example, the terminating GW has failed over to the other GK). In this case, in order for San Francisco to complete calls to San Jose, the primary GK must know to send an LRQ for the San Jose prefix to the alternate GK. Similar provisioning is required on both primary and alternate GKs to support calls in both directions.

Provisioning is also required on the DGK to prevent zone fragmentation issues when calls are originated from other zones. For example, if San Francisco sends a call to New York, the DGK does not know with which GK (primary or alternate) the NY GW is registered. The DGK must be provisioned to send sequential LRQ requests to both primary and alternate terminating local GKs for all Eastern zone supported prefixes (messages 1a and 1b, which are addressed to both DGKs in the HSRP area). Similar provisioning is required for the Western zone prefixes to support calls in the other direction.

HSRP is used to provide fault tolerance for the DGK. However, HSRP failover detection may take some time during which no calls will be processed. To cover this case, local GKs may be configured to point to more than one DGK (an ALTDGK) for its wild-card route using sequential LRQs.

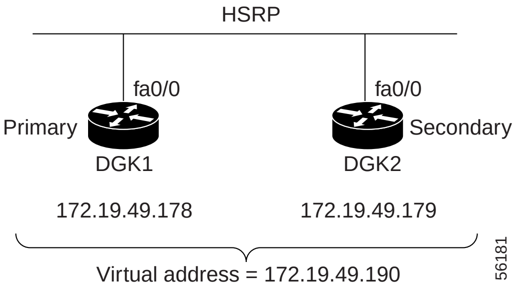
For example, the GK may point to an HSRP DGK pair as its primary option (message 1). If no response is received because HSRP failover has not been detected yet, the GK may initiate another LRQ (message 2) to an ALTDGK after a configurable timeout (100 to 1000 ms) to try to complete the call. During this time, calls will still be completed, although with additional postdial delay. The ALTDGK is configured in exactly the same way as the primary DGK HSRP pair (messages 2a and 2b).

Using HSRP on Directory Gatekeepers

Because the DGK maintains the majority of the call routing intelligence (such as zone prefix tables, tech prefix tables, E.164 registrations), the DGK should be fault tolerant. DGKs can be configured as HSRP pairs with a shared virtual IP address, so that when one DGK fails, the standby DGK assumes its role. Zone GKs need only to point to this virtual address.

A primary and secondary DGK functioning as a fault-tolerant pair must be addressed by a single virtual address. Figure 2-14 illustrates this assignment, with the virtual address 172.19.49.190 functioning as a single address (from the point of view of incoming traffic) for DGK1 and DGK2.

Figure 2-14 Assigning a Virtual Address to Paired DGKs in an HSRP Pair



An active and a standby DGK must be configured on the same subnet, and therefore must be colocated. HSRP uses a priority scheme to determine which HSRP-configured router is to be the default active router. To configure a router as the active router, you assign it a priority that is higher than the priority of the other HSRP-configured routers. The default priority is 100, so if you configure just one router to have a higher priority, that router will be the default active router.

⚠ **Caution** Cisco recommends that you use the HSRP redundancy method at the DGK level, not at the zone GK level. This is because HSRP does not support reregistration from one HSRP DGK to the adjacent HSRP DGK.

HSRP works by exchanging multicast messages that advertise priority among HSRP-configured routers. When the active router fails to send a “hello” (heartbeat) message within a configurable period of time, the standby router with the highest priority becomes the active router. An HSRP GK sends these “hello” messages every 3 seconds by default.

For more information about HSRP, refer to the following URL:

http://www.cisco.com/univercd/cc/td/doc/cisintwk/ics/cs009.htm

The standby timers interface configuration command sets the interval in seconds between hello messages (1 through 255 sec) and sets the duration in seconds that a router waits before it declares the active router to be down (1 through 255 sec). The defaults are 3 and 10 seconds, respectively. If you decide to modify the default values, you must configure each router to use the same hello time and hold time. For example, on an interface *xxx*, we could change the default values as follows:

```
int xxx
standby 1 timers 5 15
```

where 5 = hello interval and 15 = the time the active router can be down before this state is declared.

The command does not appear until the value is changed. For more information, see the topic “Configuring HSRP” at the following URL:

http://www/univercd/cc/td/doc/product/software/ios121/121cgcr/ip_c/ipcprt1/1cdip.htm

Using an Alternate Directory Gatekeeper for Fault Tolerance

HSRP failover detection may take some time, during which no calls will be processed. To cover this case, local GKs can be configured to point to an additional, or alternate, DGK. This alternate DGK can be used to back up an HSRP DGK pair, by using the sequential LRQ feature available on the zone GKs. For instance, if a zone GK sends an LRQ to a primary DGK, and fails to receive an LCF in return, another sequential LRQ can be sent from the zone GK to this alternate DGK. During this time, calls will still be completed, although with additional postdial delay. The alternate DGK will then provide the normal DGK prefix lookup and call routing in the network, until the primary DGK is able to function again. The alternate DGK is configured just like the primary DGK in the HSRP DGK pair. We apply this design in the example configuration shown in Method 3: Configuring an Alternate DGK, page 2-33.

Caution Cisco recommends that you use a combination of alternate GK, HSRP DGK, and alternate DGK to provide fault tolerance and redundancy in large H.323 networks.

Providing Redundancy for Software Upgrades

Although it is up to the service provider to determine the service availability required by its customers, it remains good practice to ensure that voice traffic is not interrupted. In many cases, “five nines” (99.999%) availability may be required. In addition to providing redundancy to cover outages of equipment or communications channels, it is necessary to provide redundancy to support traffic during upgrades of the Cisco IOS software.

Caution It is the responsibility of the service provider to engineer the network in such a way as to provide the required service availability for their customers.

Upgrading All Routers

To ensure that software upgrades do not affect service availability, Cisco recommends that you provide redundancy for all components of the GK core. Note the following considerations:

- Provide multiple GWs that service the same coverage area.
- Use alternate GKs to minimize downtime during upgrades of the Cisco IOS on a GK.
- Use alternate DGKs to minimize downtime during upgrades of the Cisco IOS on a DGK.

Note The most recent information about upgrading the Cisco IOS software can be found in the *Release Notes* for your software.

To upgrade software at the GW level, follow the steps below.

1. Ensure that the new Cisco IOS image is available on the TFTP server.
2. Download the new Cisco IOS files from a TFTP server to available flash memory on the selected routers. beforehand. To minimize service unavailability, it is recommended that you upgrade only one router at a time.

3. Select a maintenance window that ensures the least disruption of traffic. Do the following during the maintenance window.
   a. Redirect traffic from the routers whose software is to be upgraded.
   b. If you have GWs that support SS7 links, you must take those links out of service (OOS) on the Cisco SC2200 that supports those links. (This involves editing the file *config.mml* of the SC. See Step 4 of Define APCs, Linksets, SS7 Routes, and NAS Paths, page 5-13.)
   c. Reboot the routers to move the new image from flash memory to RAM. This activates the IOS upgrade.

Note Rebooting can take up to 5 minutes.

Upgrading at the Billing Component Level

It is essential that billing information not be lost. In addition to providing redundancy to cover outages of equipment or communications channels, it is necessary to provide redundancy to maintain billing data during upgrades of software to support billing applications. Components to consider include AAA/RADIUS servers, OSP servers, and other servers providing third-party billing and settlement applications.

Upgrading at the Network Management Level

It is generally not necessary to provide redundancy at the network management level, because these applications can go out of service during a maintenance window with minimal impact on traffic. However, it is the responsibility of the service provider to consider any possible effects such outages may have, and provide redundancy if necessary.

Configuring Fault Tolerance: Three Methods

The following configuration scenarios provide examples that illustrate the methods discussed above:

- Method 1: Configuring Alternate GKs
- Method 2: Configuring an HSRP DGK Pair
- Method 3: Configuring an Alternate DGK

See Figure 2-7 on page 2-11 for the relationships and address of the components discussed in these configurations.

Method 1: Configuring Alternate GKs

Use this method, which uses the **priority** statement, to configure GWs to register to a primary and secondary (alternate) GK in the absence of HSRP.

Step 1 Configure the GWs to register to an alternate GK pair. See Using Alternate Gatekeepers for Fault Tolerance, page 2-27. The following is for a single GW.

The configuration registers each GW in a zone with two GKs, one primary and one secondary. Default priority = 127 (127 is lowest priority, 1 is the highest priority). 1719 is the well-known port for H.323 RAS messaging.

```
interface Ethernet 0/1
  ip address 172.18.193.59 255.255.255.0 <----the address of this GW
  h323-gateway voip interface
  h323-gateway voip id GK1 ipaddr 172.18.193.65 1719 priority 120
  h323-gateway voip id GK1 ipaddr 172.18.193.66 1719
  h323-gateway voip h323-id cisco2
```

In this case, we have configured 172.18.193.65 as the primary (priority = 120) and 172.18.193.66 as the secondary GK.

Step 2 Verify the configuration.

```
# show gate

Alternate Gatekeeper List
 priority 120 id GK1 ipaddr 172.18.193.65 1719
 priority 127 id GK2 ipaddr 172.18.193.66 1719
```

Method 2: Configuring an HSRP DGK Pair

Use this method to configure a primary and secondary (standby) DGK in an HSRP DGK pair.

Step 1 Add an HSRP pair of DGKs, primary and secondary. See Figure 2-14 on page 2-29.

a. Configure the primary DGK, DGK1. We will use a Fast Ethernet interface.

```
interface fa0/0
  ip address 172.19.49.178 255.255.255.0
standby 1 priority 110
standby 1 ip 172.19.49.190 255.255.255.0
```

This is the actual IP address of DGK1. The next two lines declare, respectively, the standby priority for this DGK and the virtual IP address of the HSRP DGK pair.

Step 2 Declare the first DGK and create **zone local** and **zone remote** statements.

The key to establishing an HSRP pair is having identical **zone** statements on each DGK. Note the following configurations for DGK1 and DGK2, respectively. Use the **gatekeeper** command to establish the DGK identity of the router. The **zone local** statement assigns the virtual address shared by the HSRP pair.

```
gatekeeper
 zone local DGK netman.com 172.19.49.190
 zone remote NA-GK netman.com 172.19.49.168 1719
 zone remote AS-GK netman.com 172.19.49.172 1719
 zone remote E-GK netman.com 172.19.49.176 1719
 zone remote NA-AGK netman.com 172.19.49.169 1719
 zone prefix NA-GK 1*
 zone prefix E-GK 33*
 zone prefix AS-GK 86*
 lrq forward-queries
 no shutdown
```

b. Configure the secondary DGK, DGK2.

```
interface fa 0/0
  ip address 172.19.49.179 255.255.255.0
standby 1 priority 100
standby 1 ip 172.19.49.190 255.255.255.0
```

Note Note the lower standby priority. *All* **zone** statements must be *identical* to those in the other member of the HSRP DGK pair.

```
gatekeeper
 zone local DGK netman.com 172.19.49.190
 zone remote NA-GK netman.com 172.19.49.168 1719
 zone remote AS-GK netman.com 172.19.49.172 1719
 zone remote E-GK netman.com 172.19.49.176 1719
 zone remote NA-AGK netman.com 172.19.49.169 1719
 zone prefix NA-GK 1*
 zone prefix E-GK 33*
 zone prefix AS-GK 86*
 lrq forward-queries
 no shutdown
```

Method 3: Configuring an Alternate DGK

Use this method to configure an alternate DGK in the absence of HSRP. The configuration, residing on each of the zone GKs, is identical to that of the primary DGK. The following illustrates a configuration on a duplicate DGK that shares the same routing table as the primary:

```
alternate DGK
!
gatekeeper
 zone local DGK netman.com 172.19.49.190
 zone remote NA-GK netman.com 172.19.49.168 1719
 zone remote AS-GK netman.com 172.19.49.172 1719
 zone remote E-GK netman.com 172.19.49.176 1719
 zone remote NA-AGK netman.com 172.19.49.169 1719
 zone prefix NA-GK 1*
 zone prefix E-GK 33*
 zone prefix AS-GK 86*
 lrq forward-queries
 no shutdown
```

The following illustrates how to configure on each of the zone GKs a **zone remote** statement that points to an alternate DGK if the primary DGK fails. See Figure 2-13 on page 2-28, and Using an Alternate Directory Gatekeeper for Fault Tolerance, page 2-30.

Step 1 Add an alternate DGK and configure it.

```
gatekeeper
 zone local E-GK netman.com 172.19.49.176
 zone remote DGK netman.com 172.19.49.190 1719<----points to primary DGK
 zone remote ALTDGK netman.com 172.19.49.180 1719  <----points to alternate DGK
 zone prefix E-GK 3303* gw-priority 10 FRANCE-GW1
 zone prefix DGK *
 zone prefix ALTDGK *
 no shutdown
```

Providing Security

This section introduces the topic of H.235 security, and provides an example of configuring GWs, a GK, and an AAA/RADIUS server to provide security.

H.235 Security for Gateways and Gatekeepers

The RAS channel used for GW-to-GK signaling is not a secure channel. To ensure secure communication, Cisco H.235 access tokens allow GWs to include an authentication key in their RAS messages. This key is used by the GK, which passes it to a AAA/RADIUS server for verification of a user password and H.323 ID.

Cisco H.323 GWs support the use of CryptoTokens for authentication where the token can be included in the RRQ and ARQ messages. Figure 2-15 illustrates the generation and validation of a Cisco H.235 security token. This example illustrates "registration only" security. CHAP (Challenge Handshake Authentication Protocol) is the method used.

Note CHAP is supported on lines using PPP encapsulation, to prevent unauthorized access. CHAP does not itself prevent unauthorized access, but merely identifies the remote end. The router or access server then determines whether that user is allowed access.

Figure 2-15 Generation and Validation of Cisco H.235 Security Token

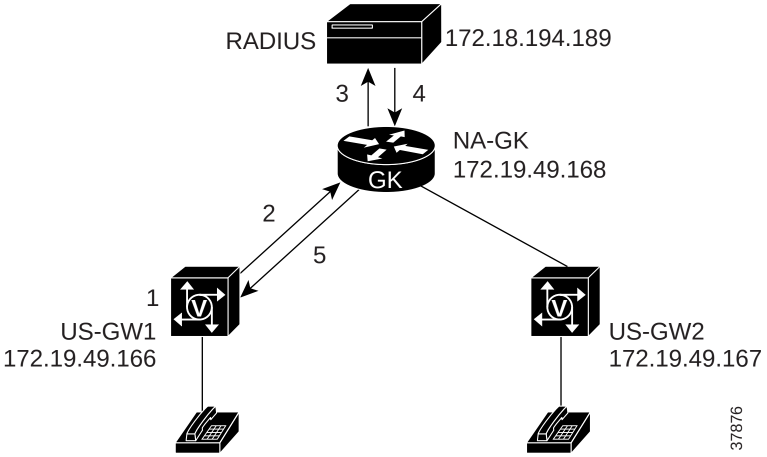
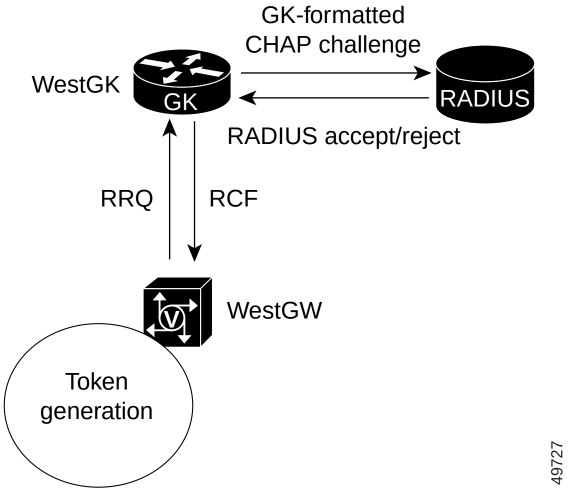


Figure 2-16 illustrates a CHAP challenge for a GW named WestGW and a GK named WestGK.

Figure 2-16 A CHAP Challenge



The general sequence is as follows:

1. A user password is manually established on the GW.
2. A token is generated at the access GW. The token results from the hashing of the user password, an H.323 ID, and a timestamp.
3. The GW passes the token to the GW as part of an RRQ (Registration Request) message.
4. The GK passes the token to the AAA/RADIUS server for validation.
    a. If the password and H.323 ID match records on the AAA/RADIUS server, the token is validated.
    b. If the password and H.323 ID do not match the records, an RRJ (Request Reject) is returned and the GW is not allowed to register with the GK.
5. The validated token is passed back to the GK as an RCF (Registration Confirm) message.

Caution The Cisco Wholesale Voice Solution supports Cisco H.235 security for *registration only*. For reasons of AAA latency, H.235 security is not supported on a per-call basis. When per-call security is required, Cisco recommends the use of access lists.

Configuring Gateways, a Gatekeeper, and an AAA/RADIUS Server for Security

The following examples illustrate security configurations for the following components:

- Two gateways, US-GW1 and US-GW2
- Their GK, NA-GK
- A AAA/RADIUS server

Refer to Figure 2-15.

US-GW1

```
hostname US-GW1
```

```
!
interface Ethernet0/0
 ip address 172.19.49.166 255.255.255.192
 h323-gateway voip interface
 h323-gateway voip id NA-GK ipaddr 172.19.49.168 1719 priority 1
 h323-gateway voip h323-id US-GW1
 h323-gateway voip tech-prefix 1#
!
gateway
security password lab level endpoint <--set password = lab (endpoint registration only)
```

US-GW2

```
hostname US-GW2
!
interface Ethernet0/0
 ip address 172.19.49.167 255.255.255.192
 h323-gateway voip interface
 h323-gateway voip id NA-GK ipaddr 172.19.49.168 1719 priority 1
 h323-gateway voip id NA-ALTGK ipaddr 172.19.49.169 1719 priority 2
 h323-gateway voip h323-id US-GW2
 h323-gateway voip tech-prefix 1#
!
gateway
```

NA-GK

```
hostname NA-GK
!
aaa new-model
aaa authentication login h323 group radius
aaa authorization exec h323 group radius
aaa accounting connection h323 start-stop group radius
!
interface Ethernet0/0
 ip address 172.19.49.168 255.255.255.192
!
gatekeeper
 zone local NA-GK netman.com 172.19.49.168
 security token required-for registration <----causes GK to check for user ID and password
 gw-type-prefix 1#* default-technology
 lrq forward-queries
 no shutdown
!
radius-server host 172.18.194.189 auth-port 1645 acct-port 1646 key lab
radius-server retransmit 3
radius-server key cisco
!
```

AAA/RADIUS Server

The configuration of the necessary files on the RADIUS host will vary according to the application. In some cases these correlate the H.323 IDs of GWs or GKs with a key, or password.

Note In some CiscoSecure applications, you will need to establish GW and GK H.323 ID (**h323-id**) values in two separate files that reside on the AAA/RADIUS host: one for users (the GWs) and one for clients (the GKs). This information resides, respectively, in two RADIUS database files in the host machine's */etc* directory: */etc/raddb/users*, and */etc/raddb/clients*.

For further details, see *RADIUS Vendor-Specific Attributes Voice Implementation Guide Version 3.0* at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/access/acs_serv/vapp_dev/vsaig3.htm

Providing Network Timing through NTP

Establishing proper timing is essential not only for the proper operation of standard network functions, but also for the establishment of accurate stop and start intervals on call legs for billing and other accounting purposes.

The information below has been adapted from Task 1. Enabling the Network Time Protocol, at the following URL:

http://www.cisco.com/univercd/cc/td/doc/cisintwk/intsolns/as5xipmo/sysmgt.htm

For further information, including NTP time formats and links to useful sites, refer to Network Time Protocol (NTP) Usage Guidelines in *Configuration Guide for AAA Billing Features in Cisco Voice-Enabled Routers and Access Servers, at the following URL:*

http://www.cisco.com/warp/public/cc/so/cuso/sp/sms/acct/caaaf_cg.htm

The Network Time Protocol (NTP) provides a common time base for networked routers, servers, and other devices. A synchronized time enables you to correlate syslog and Cisco IOS debug output to specific events. For example, you can find call records for specific users within one millisecond.

Comparing logs from various networks is essential for the following tasks:

- Troubleshooting
- Fault analysis
- Security incident tracking

Without precise time synchronization between all the various logging, management, and AAA functions, time comparisons are not possible.

An NTP-enabled network usually gets its time from an authoritative time source, such as a Cisco router, radio clock, or an atomic clock attached to a timeserver. NTP then distributes this time across the network. NTP is extremely efficient; no more than one packet per minute is necessary to synchronize two machines to within a millisecond of one another. NTP runs over UDP, which in turn runs over IP.

Note NTP services are enabled on all interfaces by default.

Configuring Additional NTP Features

There are a variety of optional NTP features you can configure. For details regarding the following options, refer to Performing Basic System Management at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/12cgcr/fun_c/fcprt3/fcgenral.htm#xtocid1345017

- Configure NTP authentication.

  Use this feature to authenticate the associations with other systems for security purposes.
- Configure NTP associations.

An NTP association can be a peer association (meaning that this system is willing to either synchronize to the other system or to allow the other system to synchronize to it), or it can be a server association (meaning that only this system will synchronize to the other system, and not the other way around). Use this feature to form an NTP association with another system.

- Configure NTP broadcast service.

  The system can either send broadcast packets or listen to them on an interface-by-interface basis. You can also use this feature to configure the estimated round-trip delay for broadcast packets.

- Configure NTP access restrictions.

  You can control NTP access by creating access groups and assigning a basic IP access list to it, and you can disable NTP services on a specific interface.

- Configure the source IP address for NTP packets.

  When the system sends an NTP packet, the source IP address is normally set to the address of the interface through which the NTP packet is sent. Use this feature to configure a specific interface from which the source IP address will be taken.

- Configure the system as an authoritative NTP server.

  Even if a particular system is not synchronized to an outside time source, you can use this feature to be an authoritative NTP server.

- Configure NTP to update the calendar.

  On systems that have calendars, you can configure NTP to update the calender periodically.

Enabling NTP on a Router

The steps below are an example of how to enable NTP on a single Cisco AS5300

Step 1 Locate an authoritative clock source. For example, you can use a Cisco router or an atomic clock that is attached to a time server.

Timesaver For testing purposes, you can use a Cisco router as the master timing source. Set the time, then assign master status to this router, as follows:

```
clock set 14:00:00 22 jun 2001
ntp master
```

However, this is not recommended in a production network.

Step 2 On the Cisco router, specify the primary NTP server's IP address and automatic calendar updates on other routers that will be slaves to the master clock:

```
!
clock set 14:00:00 30 june 2001

ntp update-calendar

ntp server 172.22.66.18 prefer
```

Step 3 Verify that the clock is synchronized to the NTP server. Inspect the status and time association. Clock sources are identified by their stratum levels. The following example shows a stratum level five clock.

```
5300-NAS# show ntp status

Clock is synchronized, stratum 5, reference is 172.22.66.18

nominal freq is 250.0000 Hz, actual freq is 250.0000 Hz, precision is 2**24
reference time is BB944312.4451C9E7 (23:11:30.266 PDT Wed Sep 22 1999)
clock offset is 0.5343 msec, root delay is 13.26 msec
root dispersion is 18.02 msec, peer dispersion is 0.09 msec
5300-NAS#
```

The following command identifies how often the NAS is polling and updating to the stratum clock. An asterisk (*) next to the NTP server's IP address indicates successful synchronization with the stratum clock.

```
5300-NAS# show ntp association


      address         ref clock     st  when  poll reach  delay  offset    disp
*~172.22.66.18      172.60.8.1       16    46    64  377     1.0    0.53     0.1
 * master (synced), # master (unsynced), + selected, - candidate, ~ configured
5300-NAS#
```

For additional information, refer to Performing Basic System Management at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/12cgcr/fun_c/fcprt3/fcgenral.htm

Interconnecting to Other Service Providers

To increase traffic volume, subscriber bases, or revenue generation, partnerships can be made between both TDM-based and IP-based telephony carriers. By interconnecting with other VoIP carriers, not only can more attractive service offerings be provided, but coverage can also be increased with a minimum investment in capital and operations.

For TDM interconnections, Cisco supports a variety of interfaces and signaling variants to provide global connectivity. For solutions not requiring SS7 signaling, see Chapter 4, "Provisioning Non-SS7-Based POPs." For solutions that require SS7 signaling, see Chapter 5, "Provisioning SS7-Based POPs."

For IP interconnections, Cisco provides high-performance call routing through standards-based methods (such as OSP and H.323v2 LRQ), while flexibly accommodating networks that are not standards-based.

The wholesale service provider has the freedom to support any combination of interconnection methods simultaneously, so as not to limit business opportunities to a particular protocol. This is not the case with closed, proprietary systems.

This section discusses the following enhancements to interconnection:

- OSP-Based Interconnection using a Clearinghouse
- LRQ Forwarding Between Directory Gatekeepers (Limited Egress CSR)

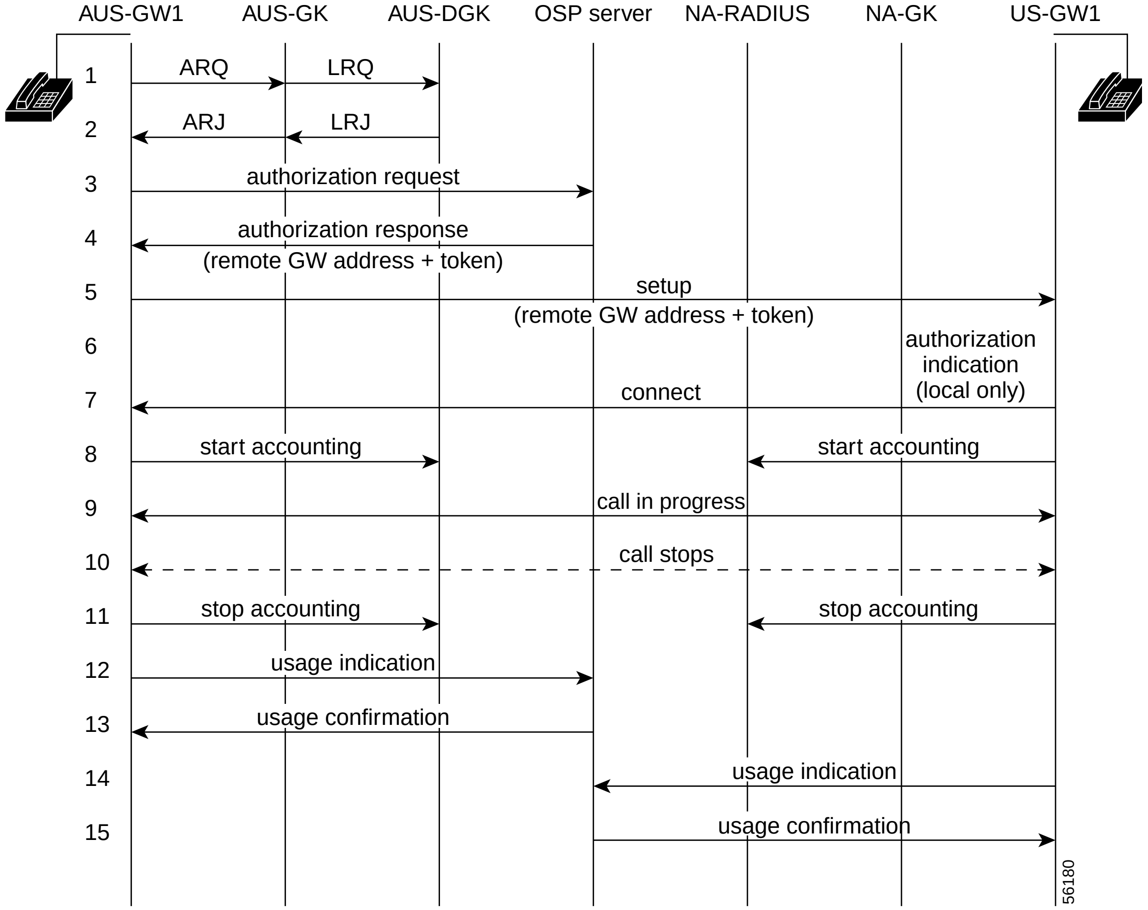
OSP-Based Interconnection using a Clearinghouse

Where multiple partners are involved and AAA/RADIUS is not used, prepaid and postpaid card services may require the assistance of clearinghouse services for billing, settlement, and invoicing. These services can be based on Open Settlements Protocol (OSP). The use of OSP for secure settlement transactions involves a clearinghouse entity, or at least a dominant carrier in the interconnect relationship that administers the OSP server. The clearinghouse maintains the OSP servers.

Note Where services are OSP based, the Cisco Wholesale Voice Solution supports call termination agreements through support for OSP in Cisco devices. For a high-level discussion of OSP, refer to Appendix A in the *Cisco Wholesale Voice Solution Overview*. For a detailed discussion of dial plans, billing/settlement, and security as these relate to OSP, see Template A3: TDM-to-IP-Based Interconnect with OSP in the *Cisco Wholesale Voice Solution Overview*.

In an OSP-based interconnect, all edge GWs must be registered with the OSP server, and rotary dial-peer failover must be provisioned to route calls through the OSP interconnect. To provide OSP-based call routing, the OSP servers hold the prefix call routing tables of all SPs that subscribe to the clearinghouse. The originating GW sends an ARQ (Authorization Request) to an OSP server, which responds with an ARP (Authorization Permit) that contains a list of possible IP addresses of the terminating GW, plus a security token. The token is included in the SETUP message, to provide security validation at the terminating GW. The SP would use the OSP method of call routing when carriers want a third party to provide the billing and settlement. Figure 2-17 illustrates an example call flow for RAS failover to an OSP server.

Figure 2-17 Example Call Flow for RAS Failover to an OSP Server



Note For information on configuring an OSP server in the network, see Provisioning OSP Servers to the Gateway, page 3-12.

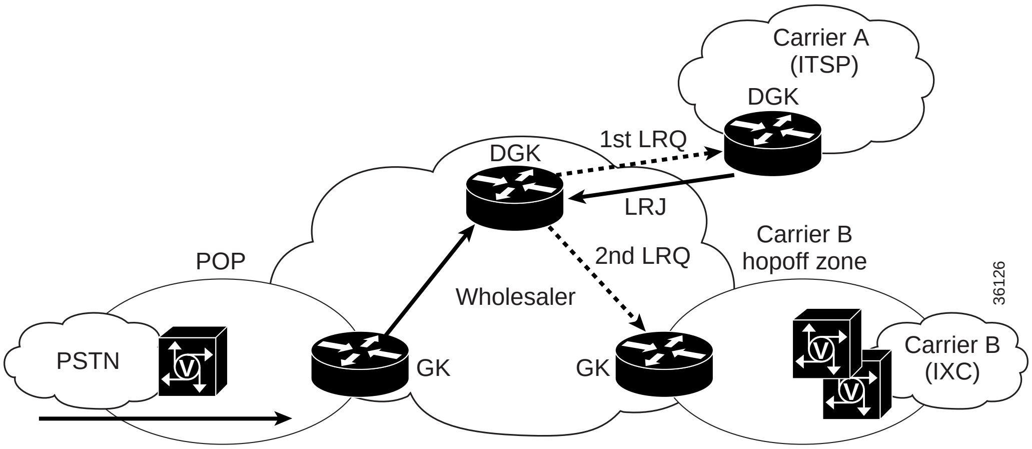
LRQ Forwarding Between Directory Gatekeepers (Limited Egress CSR)

As an added enhancement to simple carrier interconnect applications, the Cisco Wholesale Voice Solution has a limited ability to route a call to different destination carriers. This allows one service provider's DGK to send sequential LRQs (Location Requests) to other SPs' DGKs to route a call properly. The wholesaler has the same considerations as with simple carrier interconnect models, but with slightly increased call routing responsibilities.

The DGK can make limited egress carrier sensitive routing (CSR) decisions using the sequential LRQ feature. All simple, interconnect applications using DGK routing can apply this. For the most part, this consists of any TDM partners and DGK peering partners, but also includes any OSP partners where an OSP interconnection zone is used (as opposed to direct implementation on the wholesaler's GWs).

For example, the wholesaler may provision their DGKs to route certain destination-patterns to carrier A first. If carrier A is unavailable [as determined by an LRJ (Location Reject) or LRQ timeout], the wholesaler may try carrier B, then C, and so on. Figure 2-18 illustrates this application, sequential LRQ forwarding in support of limited egress CSR.

Figure 2-18 Limited Egress CSR Using Sequential LRQs



Sequential LRQ places the following restrictions on egress CSR:

- Egress carrier selection

  The gatekeeper routes calls by means of DNIS. The wholesaler statically configures a list of possible egress carriers for destinations and they are tried in order. Routing decisions are not based on which carrier sourced the call. For example, if carrier A sourced the call, it does not determine that carrier A is the first carrier selected for termination.

- Zone structure

  Each destination carrier must be contained within its own zone. For ITSP carriers interconnecting through a DGK, this is fairly simple. Interconnecting ITSPs are seen as single remote zones to which the wholesaler DGK sends LRQ messages. For interconnecting TDM carriers, this implies that the GWs capable of sending calls to the carrier are grouped into their own hopoff zone managed by a GK, and that multiple carriers are never supported on a single GW.

- No dynamic routing decisions

  Sequential LRQ selection order is statically configured. There is no provision for percentage-based routing, maximum minute cutoffs, and so on. Egress carriers are always chosen from a statically configured list of routes. If the DGK determines that an OSP interconnection zone handles a route, it is possible that the OSP server returns a terminating GW on the basis of advanced routing logic if so provisioned. For example, the OSP server may dynamically select a least-cost, terminating carrier according to criteria such as time of day or best voice quality. These options depend on the OSP server.

If OSP interconnections are supported directly from the POP GWs, sequential LRQs on the DGK may still be used to select an egress carrier through TDM or DGK peering interconnects if calls originate from any of the wholesaler POPs. If RAS fails to offer any routes, the GW may reoriginate the call through an OSP server to find termination through an IP interconnect.

For calls entering the wholesaler network from an OSP server, all POP GWs register with the OSP server. The OSP server may be provisioned with terminating carrier information and advanced routing logic rules to return the desired egress carrier GW.

Configuring a Limited CSR Application

Figure 2-19 illustrates an example network for which we will demonstrate the configuration of limited CSR. The DGK in the zone NETMAN sends LRQs sequentially to the new SP's DGKs, until the DGK zone that can route the call is found. The GK in that zone then sends an LCF confirming the route to the NETMAN GK.

We have added three new service providers in New Zealand (country code, or international calling code = 64) to our original network (see Figure 2-7 on page 2-11): ITSP-A, ITSP-B, and ITSP-C. Now look at the required configuration, which resides on the NETMAN DGK, 172.19.49.190.

We have already established the following in the provisioning we have done so far:

```
gatekeeper
zone local DGK netman.com 172.19.49.190
zone remote NA-GK netman.com 172.19.49.168 1719
zone remote AS-GK netman.com 172.19.49.172 1719
zone remote E-GK netman.com 172.19.49.176 1719
zone remote NA-AGK netman.com 172.19.49.169 1719
```

The following new three lines establish remote zones for our three new SPs:

```
zone remote ITSPA-DGK itspa.com 206.1.1.1 1719
zone remote ITSPB-DGK  itspb.com 207.1.1.1 1719
zone remote ITSPC-DGK  itspc.com 208.1.1.1 1719
```

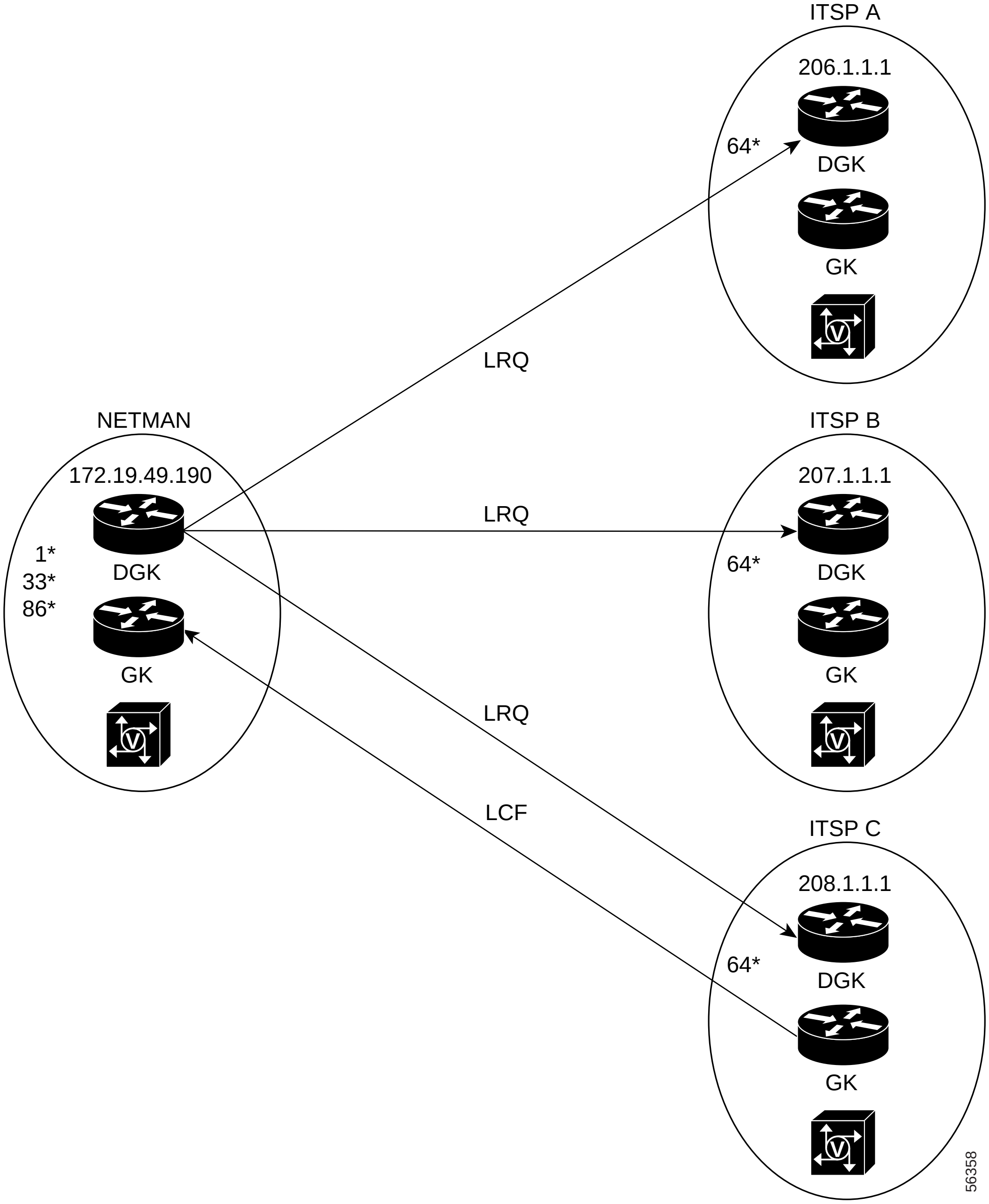
We have already established the following country code prefixes (see Table 2-2 on page 2-15):

```
zone prefix NA-GK 1*
zone prefix E-GK 33*
zone prefix AS-GK 86*
```

Now we establish the new country code prefixes for the following DGKs, and add a **zone remote** statement that directs them to the NETMAN DGK:

```
zone prefix ITSPA-DGK 64*
zone prefix ITSPB-DGK 64*
zone prefix ITSPC-DGK 64*
zone remote NA-GK netman.com 172.19.49.168 1719

 lrq forward-queries <----activates LRQ forwarding
 no shutdown
```

Figure 2-19 Example Configuration of Limited CSR



Configuring Back-to-Back Gateways

The following introductory information is borrowed in part from the *Cisco Wholesale Voice Solution Overview*, which contains additional information related to various features of back-to-back GWs. Platforms considered for back-to-back configurations are the Cisco 3600 series, the Cisco AS5300, the AS5350, and the Cisco AS5400. The Cisco 3600 series is not used where SS7 signaling is required.

Design Objective

The back-to-back GW is a special component used for a variety of applications. GWs are deployed as a pair in a back-to-back TDM T1 CAS or E1 R2 trunk, single-stage dialing configuration. Depending on the application, back-to-back GWs may function as unidirectional or bidirectional call devices.

For example, in an IVR application, the back-to-back GW has a dedicated half that receives all calls while the other half is dedicated to originating calls. In contrast, for an OSP interconnect zone application, the back-to-back GW may process calls in both directions, although each GW is responsible for separate protocols. For unidirectional applications, to provide added clarity in discussing back-to-back GW pairs, we refer to the individual GWs in a pair as an *ingress* (inbound) VoIP GW and an *egress* (outbound) VoIP GW with respect to the call direction. For bidirectional applications, we generally refer to the GW by the protocol it supports.

Figure 2-20 on page 2-46 illustrates the use of multiple back-to-back GWs within a wholesaler's network, to partition call billing among various ITSPs, an OSP clearinghouse, and a Clarent domain.

The GW pair allows wholesalers to insert themselves into the call-signaling path in IP-to-IP interconnect call topologies. This allows them to generate usage records by means of AAA, interconnect with Clarent-based and OSP-based environments, and front-end PC-to-phone applications for IP-based interconnect partners. In many ways, the back-to-back GW area functions just like a normal non-SS7 POP, with the implications discussed in the subsections that follow.

Signaling

Back-to-back GWs simply need to be configured with similar TDM signaling types. However, Cisco recommends that you use ISDN PRI signaling. Although one DS0 is lost to signaling, the call setup time is faster with ISDN (generally less than 2 seconds) than it is for T1 CAS signaling (up to 4 or 5 seconds). Use T1 or PRI crossover cables to provide the physical connection between each router.

Note The GWs in each back-to-back pair are cabled directly to each other (through T1 connections) by means of an RJ-45–to–RJ-45 T1 crossover cable.

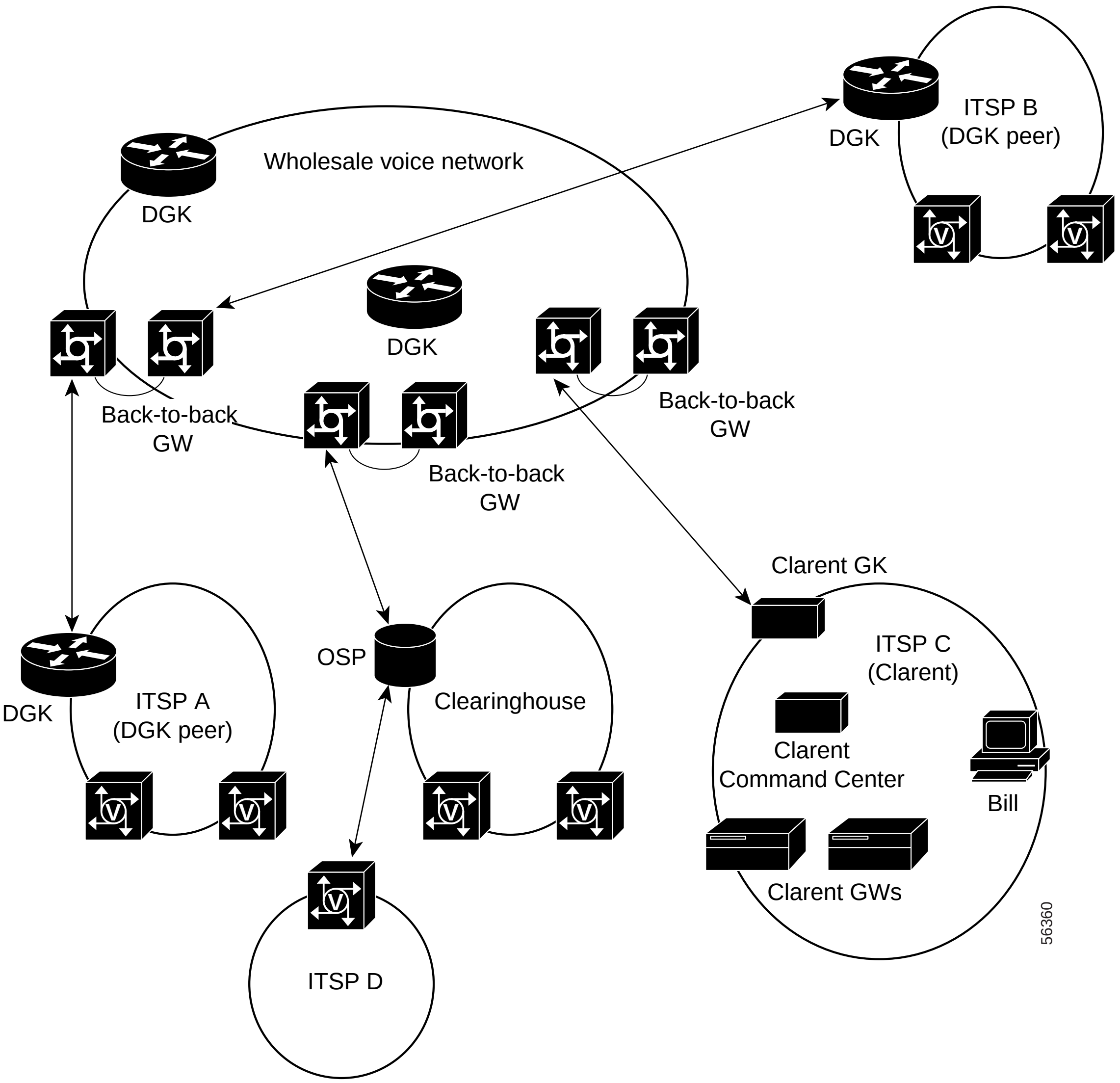
Transit Gateways

A transit GW is a back-to-back GW that acts as a proxy between an OSP clearinghouse or Clarent GK and the H.323 GK VoIP network. Transit GWs are used to enable routing by the OSP or Clarent entities without disrupting the existing H.323 network. For example, in an OSP scenario, only OSP-based calls go through the back-to-back transit GW, eliminating the need for additional OSP overhead on other GWs. The same applies in principle in a Clarent scenario.

Voice Quality/Bearer Issues

Voice quality suffers especially in the case of tandem compression. The use of back-to-back gateways adds both postdial delay and latency for all calls. There is even greater impact if more than one back-to-back GW zone is traversed. Fax relay may also suffer.

Figure 2-20 Relationship of the Back-to-Back GW to Wholesaler and Carriers



Caution Modem passthrough is highly unreliable, and as a result is not supported in scenarios that employ back-to-back GWs.

Caution Where two back-to-back GWs (that is, four routers) are used in the path of a VoIP call, the end-to-end delay can approach 250 ms, with undesirable effects on QoS. In addition, in fax calls the tones transmitted across two back-to-back GWs are not received correctly at the terminating GW, because three encode/decode sequences are involved. Consequently, Cisco recommends that no more than one back-to-back GW be used in an end-to-end call.

Configuration Examples

The following example scenarios are discussed in this section:

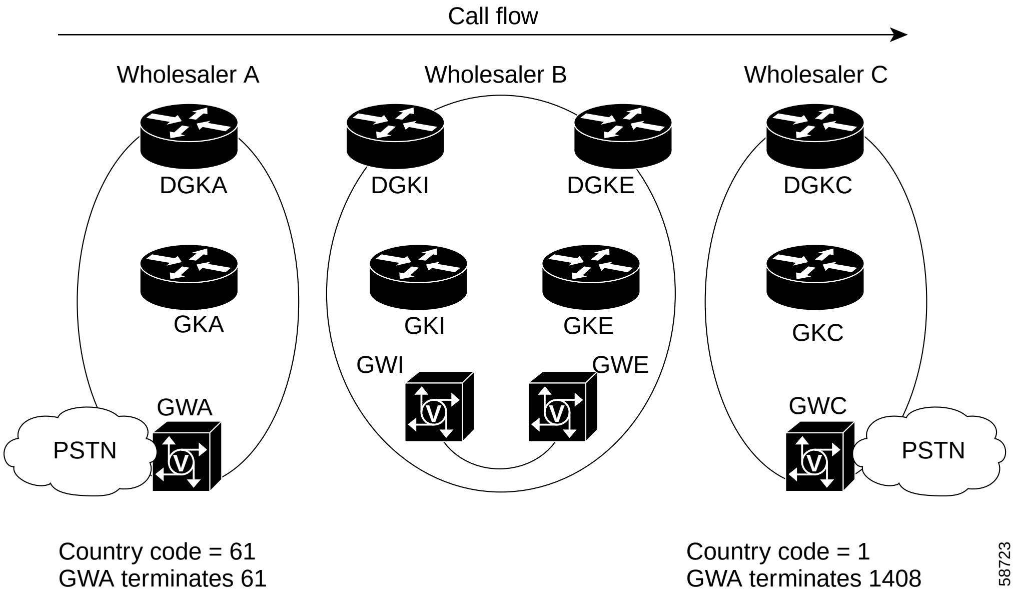
- Back-to-Back Gateway in an IP-to-IP Topology, below
- Back-to-Back Gateway in an OSP Transit Zone, page 2-51
- Back-to-Back Gateway in a Clarent Transit Zone, page 2-53
- Multiple Back-to-Back Gateways, page 2-55

Note The term *back-to-back GW* is used to refer to both GWs in the pair. This allows one to speak of multiple back-to-back GWs.

Back-to-Back Gateway in an IP-to-IP Topology

We begin with a back-to-back GW in a fundamental IP-to-IP interconnect scenario, as illustrated in Figure 2-21.

Figure 2-21 Back-to-Back GW in an IP-to-IP Topology



On the ingress side of wholesaler B’s network, wholesaler A terminates calls beginning with country code 61. On the egress side of wholesaler B’s network, wholesaler C terminates calls beginning with 1408. (*I* and *E* in wholesaler B’s network represent ingress and egress, respectively.)

The call flow is as follows:

1. Customer at 611011112222 calls 14085551111.
2. GWA is configured to forward all 1408* numbers to GWI (ingress side of back-to-back GW).
3. GWI terminates the call on the POTS side.
4. GWI reoriginates the call to GWE (egress side of the back-to-back GW).
5. GWE sends an ARQ to GKE, the GK supporting GWE, to identify the terminating GW, GWC.

The following configuration examples look at the configurations on GWI and GWE, as well as that on GWA, the originating GW.

Note Only those steps of interest to the back-to-back configuration are shown.

Ingress Back-to-Back GW: GWI

```
hostname GWI
!

!
```

Step 1 Establish the PSTN switch type. This will depend on the network to which you are interfacing, and must be the same for both the ingress and egress GW.

```
isdn switch-type primary-ni
isdn voice-call-failure 0
!
```

Step 2 Configure the T1 controller for PRI. This is the controller that will be connected to the second GW of the pair, GWE.

```
controller T1 0
 framing esf
 clock source line primary
 linecode b8zs
 pri-group timeslots 1-24
!
interface Serial0:23
 no ip address
 isdn switch-type primary-ni
 isdn protocol-emulate network
 isdn incoming-voice modem <---selects the DSP for voice
 fair-queue 64 256 0
 no cdp enable
 !
controller T1 3
 framing esf
 clock source line secondary 1
 linecode b8zs
 ds0-group 1 timeslots 1-24 type e&m-fgb dtmf dnis <---establishes DS0 group and signaling
!

interface Ethernet0
 no ip address
 shutdown
!

interface FastEthernet0
 ip address 172.19.49.76 255.255.255.128 <---the address of this GW
 duplex auto
 speed auto
 h323-gateway voip interface
 h323-gateway voip id gk-lab.cisco.com ipaddr 172.19.49.5 1719 <---ID/address of GK
 h323-gateway voip h323-id GWI.cisco.com <---H.323 ID of this GW, GWI
!
ip classless
ip route 0.0.0.0 0.0.0.0 172.19.49.1
no ip http server
```

```
!
voice-port 0:D
!
voice-port 3:1
```

Step 3 Configure the POTS dial peer to terminate 1408 calls. Because we want to preserve the entire ANI string, we use the command **no digit-strip**.

```
!
dial-peer voice 1 pots
 destination-pattern 1408.......
 no digit-strip
 port 0:D
!

!
dial-peer voice 1408 pots
 destination-pattern 1408.......
 port 0:D
 prefix 1408
!
```

Step 4 Establish the router as a GW, an essential step.

```
gateway
!
```

Egress Back-to-Back GW: GWE

```
hostname GWE
!
isdn switch-type primary-ni
isdn voice-call-failure 0
!
```

Step 1 Configure the T1 controller for PRI. This is the controller that will be connected to the first GW in the back-to-back pair, GWI.

```
controller T1 0
 framing esf
 clock source line primary
 linecode b8zs
 pri-group timeslots 1-24
!
interface Serial0:23
 no ip address
 isdn switch-type primary-ni
 isdn incoming-voice modem
 fair-queue 64 256 0
 no cdp enable
!
interface FastEthernet0
 ip address 172.19.49.77 255.255.255.128 <---the address of this GW
 duplex auto
 speed auto
 h323-gateway voip interface
 h323-gateway voip id gk-lab.cisco.com ipaddr 172.19.49.5 1719 <---ID/address of GK
 h323-gateway voip h323-id GWE.cisco.com <---H.323 ID of this GW, GWE
 h323-gateway voip tech-prefix 1#
!
ip classless
ip route 0.0.0.0 0.0.0.0 172.19.49.1
no ip http server
!
voice-port 0:D
!
dial-peer voice 2 voip
 destination-pattern 1408.......
 session target ras
!
```

Step 2 Configure the POTS dial peer for incoming calls from 61*. Again, because we do not want to send dial tone, we use the command **direct-inward-dial**.

```
dial-peer voice 61 pots
 incoming called-number 61..........
 direct-inward-dial
!
gateway
!
```

Originating GW: GWA

```
hostname GWA
!


interface FastEthernet0
 ip address 172.19.49.77 255.255.255.128
 duplex auto
 speed auto
 h323-gateway voip interface
 h323-gateway voip id gk-lab.cisco.com ipaddr 172.19.49.5 1719 <---ID/address of GK
 h323-gateway voip h323-id GWA.cisco.com <---H.323 ID of this GW, GWA
 h323-gateway voip tech-prefix 1#
```

Note For a discussion of tech prefixes, see Technology Prefixes, page 2-7.

```
!
ip classless
ip route 0.0.0.0 0.0.0.0 172.19.49.1
no ip http server
!
voice-port 0:D
!
voice-port 3:1
!
dial-peer voice 1 pots
 destination pattern 61...........  <---here is the destination pattern
 port 0:D
!
```

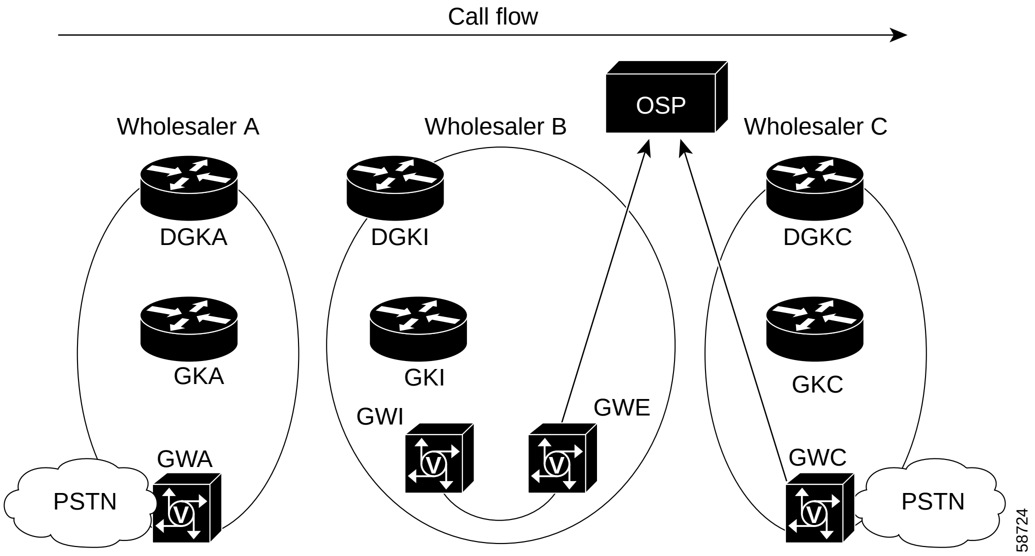
Note The first GW in the pair is configured as the session target for all calls to 1408*. Using the explicit IP address simplifies the dial plan.

```
dial-peer voice 2 voip
 destination-pattern 1408.......
 session target ipv4:172.19.49.76 <---IP address of GWI
!

!
gateway
!
```

Back-to-Back Gateway in an OSP Transit Zone

Now we look at a back-to-back GW in an OSP transit zone, as illustrated in Figure 2-22. (See Transit Gateways, page 2-45.)

Figure 2-22 Back-to-Back GW in an OSP Transit Zone



This scenario illustrates how two GWs in a back-to-back configuration can be used to create a transit zone to interconnect OSP-based networks. The ingress GW (GWI) is configured to register with the Cisco GK and acts as the demarcation point into the Cisco H.323 RAS network. The egress GW (GWE) is configured to register with the OSP server. The configuration of GWE is provided below. The configuration for GWI is not included, because it is configured as in Back-to-Back Gateway in an IP-to-IP Topology, page 2-47.

Billing CDRs for GWI are generated and reported to a RADIUS/AAA server (not shown). Billing for GWE is handled through usage indication messages sent directly to the OPS server.

The call flow is as follows:

1. Customer at 611011112222 calls 14085551111.
2. GWA is configured to forward all 1408* numbers to GWI (ingress side of back-to-back GW).

3. GWI terminates the call on the POTS side.
4. GWI reoriginates the call to GWE (egress side of the back-to-back GW).
5. GWE sends an OSP Authorization Request to the OSP server, to identify the terminating GW, GWC.

Egress GW: GWE

The following annotated configuration excerpt provides for GWE to register with the OSP server.

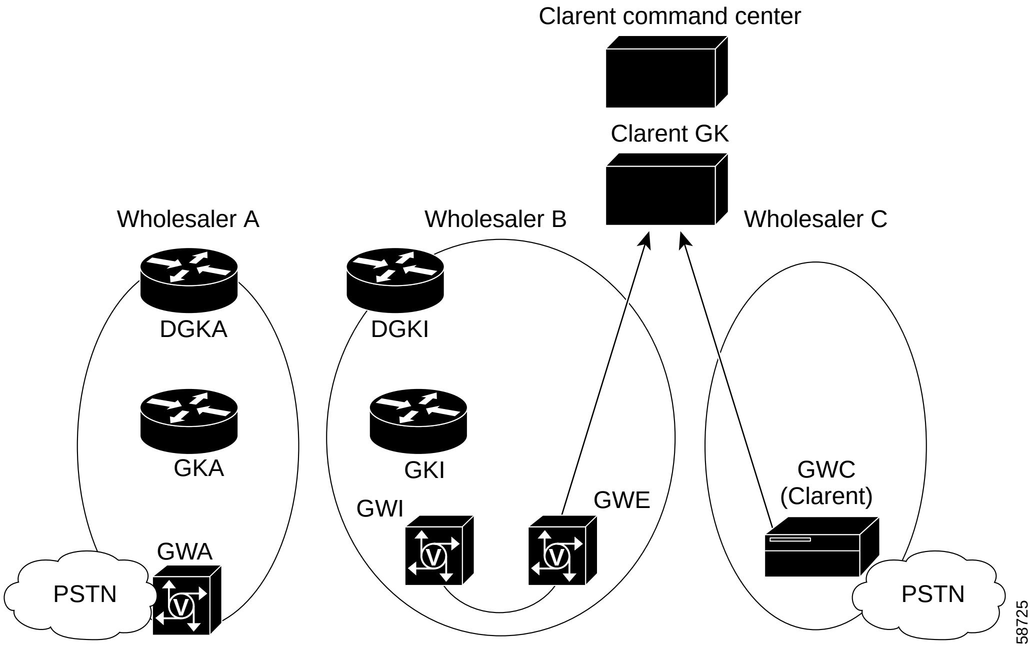
```
!
crypto ca identity OSP_clear   <---OSP_clear is the identity of the OSP server
enrollment url http://147.14.25.169:80/81   <---the protocol is HTTP; OSP server's address
crl optional
crypto ca certificate chain OSP_clear
certificate 54   <---the crypto certificate follows
30820206 3082016F A0030201 02020154 300D0609 2A864886 F70D0101 04050030
2D310B30 09060355 04061302 5553310E 300C0603 55040A13 05436973 636F310E
300C0603 55040313 056F7370 2D31301E 170D3031 30333032 32323439 30305A17
0D303230 33303232 32343930 305A303E 310B3009 06035504 06130255 53310E30
0C060355 040A1305 43697363 6F311F30 1D06092A 864886F7 0D010902 16107931
2E666965 6C646C61 62732E63 6F6D305C 300D0609 2A864886 F70D0101 01050003
4B003048 024100C3 82B4EAFD 1668C22C F1FF2609 35A63273 3D6BFC4E AE190BC3
49DC990C 6DF497F4 1799FFB9 7BD519A9 DAC8870A 2F86CDDA DB05E861 2494FD46
B8FB763B F026F102 03010001 A3693067 30090603 551D1304 02300030 0B060355
1D0F0404 030205E0 304D0603 551D1F04 46304430 42A040A0 3E863C6C 6461703A
2F2F6F73 702D312F 434E3D6F 73702D31 2C4F3D43 6973636F 2C433D55 533F6365
72746966 69636174 65526576 6F636174 696F6E4C 69737430 0D06092A 864886F7
0D010104 05000381 81003B8E 0E1809A3 76403529 FC02A523 EC8E0AFD 4A702EDB
A9CCBBB8 5CB12984 B69D8A21 3E67A122 BDD86122 7131FE55 21CA2C94 3FA689C5
52D29D31 542BB8B8 0BABD2D7 0AA054A3 5FE8A287 1DDE6504 B5D2A5FE C879BDFF
1DE9294C 6FDC9F3C 5E35126E 200D9F19 F03589A8 F810FD17 221AC2E0 848E8BEA
A03247A2 7EBA7185 289A
quit
certificate ca 01
30820258 308201C1 A0030201 02020101 300D0609 2A864886 F70D0101 04050030
2D310B30 09060355 04061302 5553310E 300C0603 55040A13 05436973 636F310E
300C0603 55040313 056F7370 2D31301E 170D3030 30393330 30313432 33375A17
0D313030 39333030 31343233 375A302D 310B3009 06035504 06130255 53310E30
0C060355 040A1305 43697363 6F310E30 0C060355 04031305 6F73702D 3130819F
300D0609 2A864886 F70D0101 01050003 818D0030 81890281 8100E009 863B2A53
B21B7F23 D8F31F70 B2E1DF69 6FA0E7C3 851BCD08 78EEA950 BBD32EDF 21B42259
7F5F31D0 B7C4EB29 A0D964C9 C0B1010E 26C202CB CE7B3E5D 8D932DD6 83EB0C32
3AD1CAF6 1FC31BB6 8DFB2851 E2568956 9BF2AA49 F61FC3FF 29A2351E BC095B87
022F4DDE FAB7A554 96C3A77C E42713EE 6CFBDE54 2CF8639C AC410203 010001A3
81873081 84301D06 03551D0E 04160414 B44E41DE 7B1A3C7E 4C3E7171 74471C72
6DAB4A57 30550603 551D2304 4E304C80 14B44E41 DE7B1A3C 7E4C3E71 7174471C
726DAB4A 57A131A4 2F302D31 0B300906 03550406 13025553 310E300C 06035504
0A130543 6973636F 310E300C 06035504 0313056F 73702D31 82010030 0C060355
1D130405 30030101 FF300D06 092A8648 86F70D01 01040500 03818100 6A43ED0F
0F9B5FBE 48DB09EE 3A6880FA 586D90F5 A848BB16 80257812 8FB7324B 6F74E3DC
BC04D29E 8621B667 DBA6EB21 62603E6B FA827425 8AF1553D 6B720F25 C11334E2
C19080AA 9F2BD742 AC01C892 471F8499 A6CE971C 59BDC184 41027F0C 878BAB36
3B29D82B 99CA360B F6D33BCA DC756927 8FE59029 70016F52 77036408
quit
!
dial-peer voice 1408 voip
destination-pattern 1408…….
session target settlement:0   <----the "settlement" matching settlement 0
!
settlement 0
type osp
url http://147.14.25.169   <---address of OSP server
encryption des-cbc-sha
```

```
no shutdown
```

Back-to-Back Gateway in a Clarent Transit Zone

This is similar to our previous example, except that now a Clarent GK and associated Clarent Command Center replace the OSP server. See Figure 2-23.

Figure 2-23 Back-to-Back GW in a Clarent Transit Zone



This scenario describes how a back-to-back GW can be used to create a transit zone when interconnecting with Clarent-based networks. The ingress GW (GWI) is configured to register with the Cisco GK and acts as the demarcation point into the Cisco H.323 RAS network. The second B2B GW (GWE) is configured to register with the Clarent GK, which supports H.323 on one side and Clarent proprietary protocol on the other. The configuration of the egress GW, GWE, is provided below. The configuration for GWI is not included, because it is configured as in Back-to-Back Gateway in an IP-to-IP Topology, page 2-47.

GWE will look essentially like another GW to the Clarent Command Center, and CDRs will be generated through the same GK Routed Call Signaling (GKRCS) methods that Clarent supports.

The call flow is as follows:

1. Customer at 611011112222 calls 14085551111.
2. GWA is configured to forward all 1408* numbers to GWI (ingress side of back-to-back GW).
3. GWI terminates the call on the POTS side.
4. GWI reoriginates the call to GWE (egress side of the back-to-back GW).
5. GWE sends an ARQ to the Clarent GK, to identify the terminating GW, GWC.

Egress GW: GWE

The following annotated configuration excerpt provides for GWE to register with the Clarent GK.

```
hostname GWE
!
isdn switch-type primary-ni
isdn voice-call-failure 0
!
```

Step 1 Configure the T1 controller for PRI. This is the controller that will be connected to the ingress GW, GWI.

```
controller T1 0
 framing esf
 clock source line primary
 linecode b8zs
 pri-group timeslots 1-24
!
interface Serial0:23
 no ip address
 isdn switch-type primary-ni
 isdn incoming-voice modem
 fair-queue 64 256 0
 no cdp enable
!
interface FastEthernet0
 ip address 172.19.49.77 255.255.255.128
 duplex auto
 speed auto
 h323-gateway voip interface
 h323-gateway voip id gk-lab.cisco.com ipaddr 172.19.49.5 1719
 h323-gateway voip h323-id GWE.cisco.com
 h323-gateway voip tech-prefix 1#
!
ip classless
ip route 0.0.0.0 0.0.0.0 172.19.49.1
no ip http server
!
```

Step 2 Use a translation rule such as the one below to translate the 1408 * to a national number type, which is the Clarent default.

```
translation-rule 1
  rule 1 ^1408....... 1408 ANY national

!
voice-port 0:D
!
dial-peer voice 2 voip
 destination-pattern 1408.......
 session target ras
 translate outgoing-called 1
!
```

Step 3 Configure the POTS dial peer for incoming calls from 61……… Because we do not want send dial tone, we use the command **direct-inward-dial**.

```
dial-peer voice 61 pots
 incoming called-number 61........
 direct-inward-dial
!
gateway
```

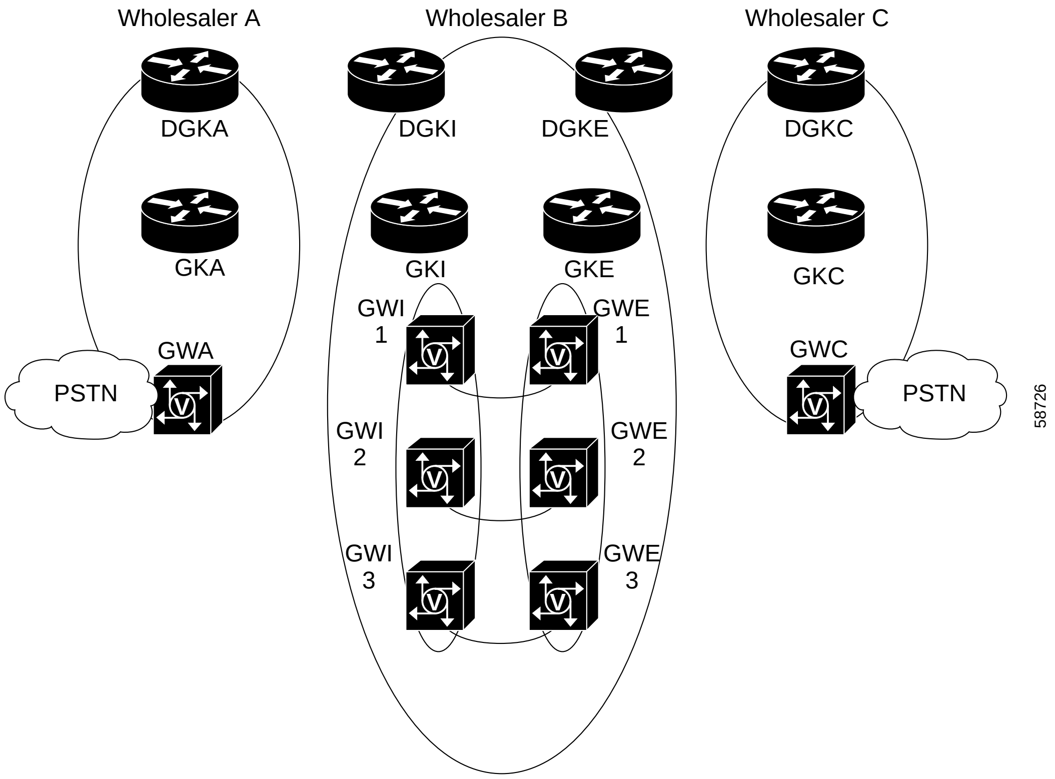
```
!
```

Multiple Back-to-Back Gateways

Finally, we consider the case of multiple back-to-back GWs. Where traffic requirements are high, these provide more than one TDM interface worth of simultaneous calls. Figure 2-24 illustrates this topology. The basic issues to consider are the following:

1. Configure the ingress and egress GWs in the back-to-back pair as in Back-to-Back Gateway in an IP-to-IP Topology, page 2-47.
2. Use dial peers to groom the traffic you want assigned to each back-to-back GW.

Figure 2-24 Multiple Back-to-Back GWs



Establishing Core Components

This section discusses the following installation and provisioning topics:

- Establishing Gateways, page 2-59
- Establishing Gatekeepers, page 2-62
- Establishing Directory Gatekeepers, page 2-63

Timesaver Because it depends on many components, the Cisco Wholesale Voice Solution depends upon many documents. As noted in Related Documents, page x, you can access these documents directly from the electronic version of this guide by clicking on the URL. The following sequence will help you navigate to where these documents reside on Cisco's public website, http://www.cisco.com/univercd/home/home.htm.

Before proceeding, however, you may find it useful to size your network, as discussed in the section below.

Determining Numbers of Components

Sizing your network, or determining the number of components of a certain type to serve a given architecture, is not an exact science. However, there are general guidelines that provide good first-order estimates. The following discussion will help you estimate approximate numbers for the following relationships:

- Number of POPs Required, page 2-56
- Number of GWs Required per POP, page 2-56
- Number of GKs Needed to Support the GWs, page 2-58
- Number of DGKs Needed to Support the GKs, page 2-58

Number of POPs Required

POPs are locally defined entities that serve both common prefixes as well as distinct geographical serving areas. It is the responsibility of the service provider to determine the number and location of POPs that will partition the wholesale network to accommodate anticipated traffic.

Number of GWs Required per POP

Consider the following in designing the service provider POP:

- Busy Hour Call Attempts (BHCA)
- The number of GWs required to handle the anticipated call volume
- The number of GKs required to process the GW signaling and RAS messaging (this is the number of zones)

The BHCA supported per platform depends on the following factors:

- platform model
- fault-tolerance features

- number of registered endpoints
- dial plan complexity
- average hold times

However, the majority of these factors are beyond the scope of the following discussion.

First consider the maximum number of BHCA a given POP must support during the busiest time of day. The general formula is as follows:

*POP BHCA = Max POP CPS * 60 * 60*

where *POP BHCA* is the peak traffic the entire POP must support, *Max POP CPS* is the maximum anticipated calls per second for the *entire POP*, and 60 * 60 is the number of seconds per minute times the number of minutes per hour. A good working number for *Max POP CPS* at peak calling periods is 5, which we use in our examples.

Next consider the BHCA per DS0. The general formula is as follows:

DS0 BHCA = (60/HT)

where *DS0 BHCA* is the maximum number of DS0s per hour supported, 60 is the number of minutes per hour, and *HT* is hold time.

Thus, for an *HT* of 3, we obtain a *DS0 BHCA* of 20.

Now we need to know the BHCA for a given GW, the *GW BHCA*. However, the maximum number of DS0s per GW depends not only on the GW but also on the signaling type. Table 2-3 presents sizing parameters for the four common signaling types, for a Cisco AS5300. That router supports a typical maximum call rate of 2 CPS, a maximum of 92 T1 DS0s, and a maximum of 120 E1 DS0s. Numbers in parentheses indicate both origination and termination.

Table 2-3 Sizing Parameters per Signaling Type, for a Cisco AS5300

Parameter	T1 PRI	T1 CAS	E1 PRI	E1/R2
GW BHCA	1840[1]	1920	2400[2]	2400
Number of GWs	544 (1088)	521 (1042)	417 (834)	417 (834)
Number of Zones	6 (12)	6 (12)	5 (10)	5 (10)

[1] 92 * 20 BHCA per DS0

[2] 120 * 20 BHCA per DS0 (0.67 CPS)

If we assume a *Max POP CPS* of 5 in our example POP, we obtain a *POP BHCA* of 18,000. Now we need to know the number of GWs we need to support this call rate. The general formula is as follows:

Number of GWs = (POP BHCA)/(GW BHCA)

So, if we take an E1 example, we have a *GW BHCA* of 2400, resulting in

Number of GWs = (POP BHCA)/2400)

= 18,000/2400

= 7.5 GWs needed to support a BHCA of 18,000

= 8 GWs needed

(Fractional GWs are not practical.)

Note However, at this point you may wish to reassess your traffic requirements in favor of saving a GW if possible.

Number of GKs Needed to Support the GWs

Now we proceed to estimating the number of GKs needed to support our GWs. With a Cisco 7200 GK, call success rates of 99% have been seen with 1000 registered endpoints (GWs) at 60 CPS (that is, 60 transactions with the GK per second during peak calling periods). We must ensure that this rate is not exceeded given the number of GWs being served by the GK and the CPS those GWs can handle. In other words, we are looking for a maximum GK CPS (*Max GK CPS*) that is below 60.

Note For the Cisco 3660 as a GK, call success rates of 99% have been seen with 1000 endpoints at 40 CPS.

The following calculations are for a single POP. Here we must consider the maximum CPS for a GW, which we will call *Max GW CPS*. This figure varies according to platform, but here we will again assume a *Max GW CPS* of 2 for the Cisco AS5300. *Max GK CPS* is a function of the number of GWs. The general formula is as follows:

*Max GK CPS = Number of GWs * Max GW CPS*

For a single POP with the 8 GWs we derived previously, this is

*Max GK CPS= 8 * Max GW CPS*

= 8 * 2

= 16 CPS maximum to support a BHCA of 18,000

If we have three symmetrical POPs with 8 GWs each to service an SP network, can we service them with a single GK? Three POPs places a load on the GK of 3 * 16 = 48 *Max GK CPS*—clearly within our recommended limit of 60 *Max GK CPS*. With asymmetrical POPs, simply count the total number of GWs you need to serve by a single GK, and ensure that you do not exceed 60.

Note Theoretically, you could therefore support up to 30 (2 * 30 = 60) Cisco AS5300 GWs with a single Cisco 7200 GK.

Number of DGKs Needed to Support the GKs

Finally, we need to determine how many DGKs we will need to support our GKs. The key factor here is CPU load. The following rough guidelines have been established through testing:

- Do not exceed a CPU load of 65%.
- 100% of new calls on a GK interact with the DGK. For a call rate of 60 CPS, each GK uses from 8 to 10% of the DGK's CPU.
- For GKs that forward 100% of new calls to a DGK, 6 GKs will use 60% of the DGKs CPU, for a GK/DGK CPU load ratio of 6:1.
- The total GK RAS messaging sent to the DGK is estimated to be 20% of the total RAS messaging in the network.

Caution Cisco recommends that you adhere to a GK/DGK ratio of 6:1. Also take into account that typical DGK deployments handle less than 100% of new calls, and that GK/DGK ratios will increase.

In a service provider network with three symmetrical POPs with 8 GWs each, we have a total of 3 GKs, clearly within the GK/DGK ratio of 6:1. However, the recommended 6:1 GK/DGK ratio is for 100% new calls. For a call load of 20% of that, we can have a 30:1 ratio of GKs to DGKs:

(1/0.2) * 6 = 30

Establishing Gateways

If your application *does not require* SS7 signaling, the GW provisioning discussed below is sufficient. If SS7 signaling is required, refer to Chapter 5, "Provisioning SS7-Based POPs."

Selecting the Appropriate Gateway

Refer to Table 2-4 for the following discussion.

Table 2-4 Cisco VoIP Gateways, Interface Modules, and Supported Signaling Types

Platform	Interface Modules	Signaling Types
Cisco 3600 series GWs (Cisco 3620, Cisco 3640, Cisco 3660)	NM-2V • Analog FXO WIC • Analog E&M WIC • BRI WIC	Analog FXO ground start, loop start, immediate start Analog E&M types I through V BRI (ETSI, NI-2)
	NM-HDV-1 T1/E1 NM-HDV-2 T1/E1 T1/E1 WVIC	PRI (ETSI, NI-2) T1 CAS (FGB[1], FGD) E1 R2 E1 R2—MF
Cisco AS5300, Cisco AS5350	Quad T1 Quad E1	PRI (ETSI, NI-2) T1 CAS—(FGB, FGD) E1 R2 E1 R2—MF Cisco SS7 Interconnect for Voice Gateways (Q.767, TR-113, China TUP)
Cisco AS5400	Octal T1/E1	CT1/CE1/PRI (ETSI, NI-2) T1 CAS (FGB, FGD) E1 R2 E1 R2—MF DS3 Cisco SS7 Interconnect for Voice Gateways (Q.767, TR-113, China TUP)

1. FG = feature group

Follow the steps below to establish GWs and interfaces appropriate to your network.

Note For the latest information, always visit the website that supports your Cisco equipment.

Step 1 Determine the types of GWs you will use. Refer to the Platform column in Table 2-4.

a. For Cisco 3620, 3640, and 3660 GWs, see Procedures for Cisco 3600 Series Gateways, page 2-60.

b. For Cisco AS5300 series GWs, see Procedures for Cisco AS5300 Gateways, page 2-60.

c. For Cisco AS5350 and Cisco AS5400 GWs, see Procedures for Cisco AS5350 and Cisco AS5400 Gateways, page 2-61.

Step 2 Determine the signaling types required for each interface you need to support. This will depend on your telephony service provider. Refer to the Signaling Types column in Table 2-4.

Step 3 Determine the types of interface cards required to support the required signaling. Refer to the Interface Modules column in Table 2-4.

Step 4 Install and provision the interface cards as needed, considering the following parameters:

a. For Cisco 3620, Cisco 3640, and Cisco 3660 GWs, see Procedures for Cisco 3600 Series Gateways, page 2-60.

b. For Cisco AS5300 series GWs, see Procedures for Cisco AS5300 Gateways, page 2-60.

c. For Cisco AS5400 GWs, see Procedures for Cisco AS5350 and Cisco AS5400 Gateways, page 2-61.

Step 5 When you are done you will have established the necessary access GWs. Now refer to the following:

a. To establish GKs, see Establishing Gatekeepers, page 2-62.

b. To establish DGKs, see Establishing Directory Gatekeepers, page 2-63.

Procedures for Cisco 3600 Series Gateways

Follow the steps below to access the necessary documentation:

1. Refer to the following: *Cisco 3600 Series Routers* at

   http://www.cisco.com/univercd/cc/td/doc/product/access/acs_mod/cis3600/index.htm

2. If you have not yet installed this equipment, begin with the following series of documents at the above URL:
   - *Cisco 3660 Router Cabling and Setup Quick Start Guide*
   - *Cisco 3600 Series Hardware Installation Guide*
   - *Cisco Network Module Hardware Installation Guide For Cisco 2600 Series and Cisco 3600 Series Routers*

Procedures for Cisco AS5300 Gateways

Follow the steps below to access the necessary documentation:

1. Refer to the following: *Cisco AS5300* at

   http://www.cisco.com/univercd/cc/td/doc/product/access/acs_serv/5300/index.htm

2. If you have not yet installed this equipment, begin with the following series of documents at the above URL:
   - *Cisco AS5300 Quick Start Guide (with Fast Step)*
   - *Cisco AS5300 Chassis Installation Guide*
   - *Cisco AS5300 Module Installation Guide*
   - *Cisco AS5300 Software Configuration Guide*

Procedures for Cisco AS5350 and Cisco AS5400 Gateways

Follow the steps below to access the necessary documentation:

1. Refer to the following: *Cisco AS5400* at

   http://www.cisco.com/univercd/cc/td/doc/product/access/acs_serv/as5400/index.htm
2. If you have not yet installed this equipment, begin with the following series of documents at the above URL:
   - *Cisco AS5400 Universal Access Server Read Me First*
   - *Cisco AS5400 Chassis Installation Guide*
   - *Cisco AS5350 and Cisco AS5400 Universal Gateway Card Installation Guide*
   - *Cisco AS5350 and Cisco AS5400 Software Configuration Guide*

Establishing Gatekeepers

The Cisco Wholesale Voice Solution uses Cisco 3640, Cisco 3660, and Cisco 7200 routers as GKs.

Selecting the Appropriate Gatekeepers

Your selection of Cisco hardware to function as GKs will depend on the traffic needs of your network.

Procedures for Cisco 3600 Series (Cisco 3640, Cisco 3660) Gatekeepers

See Procedures for Cisco 3600 Series Gateways, page 2-60.

Procedures for Cisco 7200 Gatekeepers

Depending on which router you have selected (Cisco 7202, Cisco 7204, or Cisco 7206), follow the steps below to access the necessary documentation:

Cisco 7202

1. For the Cisco 7202, refer to the following:

   Cisco 7202 at

   http://www.cisco.com/univercd/cc/td/doc/product/core/7202/index.htm

2. If you have not yet installed this equipment, begin with the following document at the above URL:

   Cisco 7202 Installation and Configuration Guide

Cisco 7204

1. For the Cisco 7204, refer to the following:

   Cisco 7204 at

   http://www.cisco.com/univercd/cc/td/doc/product/core/7204/index.htm

2. If you have not yet installed this equipment, begin with the following document at the above URL:

   Cisco 7204 Installation and Configuration Guide

Cisco 7206

1. For the Cisco 7206, refer to the following:

   Cisco 7206 at

   http://www.cisco.com/univercd/cc/td/doc/product/core/7206/index.htm

2. If you have not yet installed this equipment, begin with the following document at the above URL:

   Cisco 7206 Installation and Configuration Guide

Establishing Directory Gatekeepers

DGKs are an optional, not mandatory, component of the Cisco Wholesale Voice Solution. However, they are required in large-scale H.323 VoIP networks. The Cisco Wholesale Voice Solution uses Cisco 3640, Cisco 3660, and Cisco 7200 routers as DGKs. The Cisco 3620 is not appropriate for this purpose.

Selecting the Appropriate Directory Gatekeeper

Your selection of Cisco hardware to function as DGKs will depend on the traffic needs of your network.

Procedures for Cisco 3600 Series Directory Gatekeepers

See Procedures for Cisco 3600 Series Gateways, page 2-60.

Procedures for Cisco 7200 Directory Gatekeepers

See Procedures for Cisco 7200 Gatekeepers, page 2-62.

CHAPTER 3

Provisioning Shared Support Services

Introduction

Whereas the infrastructure of the TDM-based PSTN essentially has billing mechanisms built in, VoIP networks require their own reliable billing mechanisms to account for call start and stop times across the various call legs, or definable sections of a call's path. Where multiple service providers are involved in a Cisco Wholesale Voice Solution, tools and applications that cross SP boundaries become essential. These are known as shared support services, and have a major role in ensuring that billing is performed correctly and call time records are apportioned appropriately among the various SPs involved in a call's transit.

This chapter discusses issues that are essential to understanding these shared services, and provides configuration examples. The features available in the H.323 standard for packet telephony provide for billing from the GW by using the accounting component of AAA/RADIUS capabilities.

This chapter presents the following major topics related to billing:

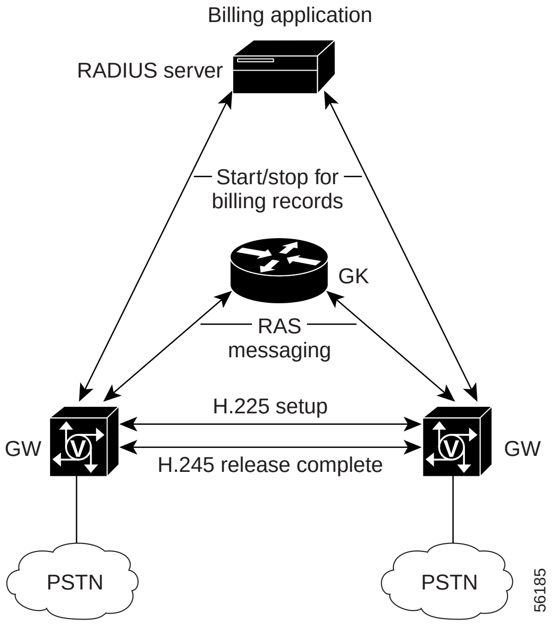
- Understanding and Provisioning AAA Billing
- Provisioning OSP Servers to the Gateway
- Establishing Billing Systems for Calling Card Services
- Provisioning Services to Support IVR
- Clarent Clearinghouse Services

In addition, management applications become critically important when networks become large. See the following for an overview of how to install and use such systems:

- Using Network Management Applications

Figure 3-1 illustrates the relationship between originating and terminating GWs, their shared GK, and a RADIUS server. In effect, during a call setup both GWs communicate with the RADIUS server and the GK, in addition to each other. (See Figure 3-2 on page 3-3.)

Figure 3-1 Relationship between GWs, GK, and RADIUS Server



Understanding and Provisioning AAA Billing

The following discussion draws from the following document:

Configuration Guide for AAA Billing Features in Cisco Voice-Enabled Routers and Access Servers, at the following URL:

http://www.cisco.com/warp/public/cc/so/cuso/sp/sms/acct/caaaf_cg.htm

Note Refer to the above website for more detail and configurations. However, more current provisioning information related to RADIUS attribute fields is presented in the following discussion.

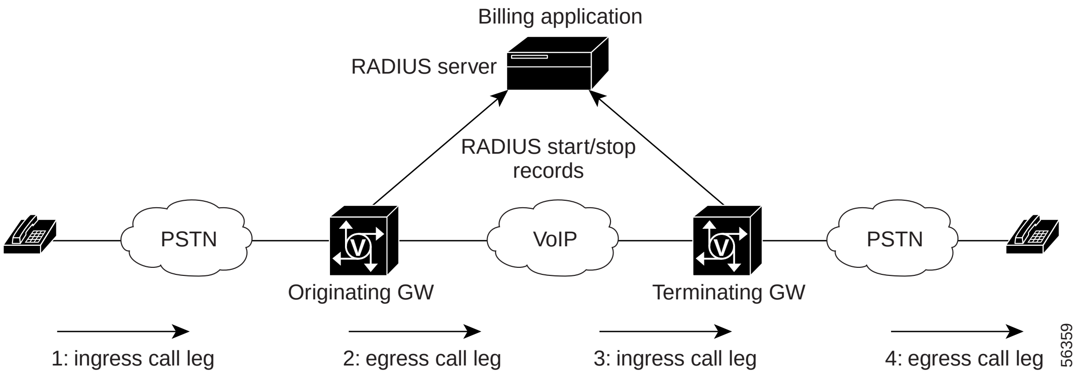
The accounting features in the AAA framework of the Cisco IOS software aid in the development of third-party billing systems, specifically for voice-enabled access servers and routers. Although AAA represents authentication, authorization, and accounting, only the accounting element of AAA and the RADIUS A/V (attribute/value) pairs generated through its use are addressed here. This Cisco IOS software and RADIUS accounting feature is required in VoIP gateways for producing accurate and timely billing and usage information.

The Foundation of Billing: The Call Leg

Cisco IOS accounting for voice uses standard RADIUS attributes where possible. There are two fundamental accounting methods. For an explanation and recommendations, see Methods to Enable VoIP Accounting on Gateways to Support Billing, page 3-6. Essential to billing is the call leg, one of four discrete paths from one PSTN subscriber to another. Figure 3-2 illustrates the four call legs between the ingress and egress PSTN:

1. First ingress leg, from the PSTN subscriber to the originating GW
2. First egress leg, from the originating GW to the VoIP network
3. Second ingress leg, from the VoIP network to the terminating GW
4. Second egress leg, from the terminating GW to the PSTN subscriber

Figure 3-2 Call Legs and Records



Data are collected for each call leg that is created on the GW. A call leg is the internal representation of a connection to the GW. Each connection that is made through the GW consists of two call legs: an incoming (answer) and an outgoing (originate) call leg. A connection using an originating and a terminating GW has four separate call legs (answer telephony, originate VoIP, answer VoIP, and originate telephony). When start-stop accounting is used, there is a separate start record and stop record for each call leg. This implies that a call generated between two voice-enabled routers will generate four discrete start records and four discrete stop records for each call connected, all having the same connection (or conference) ID (refer to Table 1, Standard Supported RADIUS Attributes, in *Configuration Guide for AAA Billing Features in Cisco Voice-Enabled Routers and Access Servers*). The various call-leg records for a single end-to-end call can be correlated through the *VSA conf_id* (conference ID; attribute name = h323_conf_id) field, a 128-bit field in hexadecimal format.

Call start and stop records are sent to the RADIUS host from each GW. Each call leg generates *start*, *update*, and *stop* records, and each record has information specific to its call leg. Each leg reports the NTP (Network Time Protocol) time for each of the following states:

- The time at which the SETUP (*start*) is issued (the start record)
- The time at which the call is connected (*update*) (the update record)
- The time at which the DISCONNECT (*stop*) is received (the stop record)

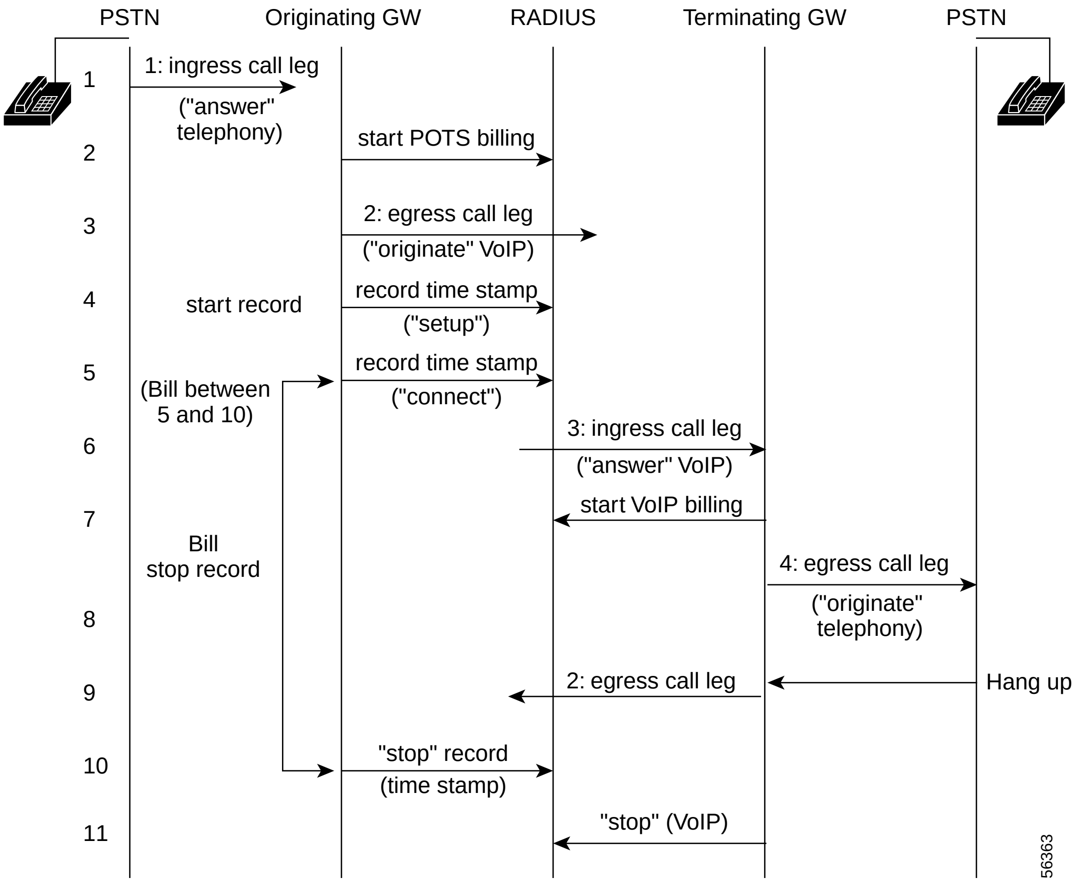
Caution Although the start record for each leg may be useful for diagnostic purposes, do not use it for billing. As a general rule on GWs, Cisco recommends that you bill at call legs 2 and 3, using the stop record. This will cover approximately 90% of the cases. However, circumstances will arise that require billing at other parts of the network, depending on the path a call must make before it terminates.

Note NTP is discussed in Using Network Time Protocol (NTP), page 3-10.

AAA accounting in Cisco IOS software for voice calls can be configured to record either *start-stop* or *stop-only* records. The *start-stop* option creates a record for each call leg at the start of a call and at the end of the same call. The *stop-only* option just creates the records for all call legs at the end of each call. If *stop-only* accounting is configured, then the number of records generated for one call would be four (a stop record for each of the four call legs). The various call leg *start* and *stop* records generated by the GWs can be organized by their conference ID, which is the same for all call legs of a connection. Using the connection ID value as the glue, a billing application can generate all the information needed for accurate and timely billing.

Figure 3-3 illustrates the call leg events and recommended billing interval for RADIUS billing.

Figure 3-3 Call Leg Events for RADIUS Billing



Configuring AAA Accounting

There are four fundamental steps to configuring AAA in a configuration session:

1. Enable AAA on the GW.
2. Define the accounting methods.
3. Define the RADIUS server.
4. Establish key files on the RADIUS server.

The above and other issues are covered under the following topics:

- Configuring a Gateway for AAA, page 3-7
- Establishing Essential Files on the RADIUS Server, page 3-10

For an example configuration, see Configuring a Gateway for Prepaid Card Service, page 3-16. Before proceeding to that section, it will be beneficial to understand issues related to voice prompts and billing, as discussed in the following:

- Provisioning Services to Support IVR, page 3-19
- Establishing Billing Systems for Calling Card Services, page 3-15

AAA Accounting Commands

The following Cisco IOS commands are designed for configuring the service provider voice over IP accounting and billing functionality.

```
aaa accounting connection h323 <stop-only | start-stop> group radius
```

This configuration defines the accounting method list "h323" with RADIUS as a protocol and with either *stop-only* or *start-stop* accounting options. The method list must be called *h323* and is activated for all voice interfaces. This command tells the system to use a method list called *h323*, which has *start-stop* or *stop-only radius* as its method. The *h323* method list is static and is applied by default to all voice interfaces.

Note The **group** command is required.

Accounting Command References

For a complete description of Cisco accounting commands and their parameters, see Accounting Commands under *Authentication, Authorization, and Accounting* at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/secur_r/srprt1/index.htm

The above is part of the *Cisco IOS Security Command Reference, Release 12.1*.

For details on using the AAA accounting commands, refer to Cisco IOS AAA Accounting Commands in *Configuration Guide for AAA Billing Features in Cisco Voice-Enabled Routers and Access Servers*, at the following URL:

http://www.cisco.com/warp/public/cc/so/cuso/sp/sms/acct/caaaf_cg.htm.

Debug and troubleshooting commands are provided there also, in addition to the following topics:

- The Anatomy and Dissection of a Call Detail Record
- RADIUS Accounting Records
- Example Session for Exporting RADIUS Records in CiscoSecure UNIX v 2.3

- Call Leg Accounting Records for Four Different Calls
- Analysis of Call Records
- Router Configurations and Versions

Methods to Enable VoIP Accounting on Gateways to Support Billing

There are two ways to enable accounting on GWs to support billing. Until Cisco IOS Release 12.0(7)T, the Cisco specific parameters were overloaded into RADIUS attribute 44, Acct-Session-ID. Attributes that cannot be mapped to standard RADIUS are "packed" into the *Acct-Session-Id* attribute field (attribute 44) as a "/" (forward slash) delimited ASCII string. The older method has been superseded by a newer, recommended method: using vendor-specific attributes, or VSAs. Both methods are discussed below.

Recommended Method: Enabling Cisco VSAs in RADIUS Attribute 26

Attribute 44 carries a limited amount of information. Enabling attribute 26 makes a larger set of information available for communication. In releases later than Cisco IOS Release 12.0(7)T, the overloaded Acct-Session-ID method continues to be the GW's default behavior, but you can configure the GW to enable VSAs. (VSAs are platform-independent and comply with voice platforms supported by Cisco.) When you enable accounting, this default behavior is enabled.

To enable gateway-specific VSAs, use the commands **radius-server** and **gw-accounting** in global configuration mode. The two fundamental steps are as follows:

1. Enable the GW to recognize and use VSAs as defined by RADIUS attribute 26. This establishes communication between the GW and the server.

   ```
   radius-server vsa send [accounting | authentication]
   ```

2. Enable GW-specific accounting.

   ```
   gw-accounting h323 vsa
   ```

The option **h323** configures standard H.323 accounting by means of standard IETF RADIUS attributes. This enables call data records (CDRs) to be generated for voice calls. The option **vsa** enables H.323 accounting through RADIUS vendor specific attributes.

Note The command **gw-accounting** also provides a **syslog** option. The **syslog** keyword configures the system logging facility to output accounting information in the form of a system log message. For more information about this type of accounting, see Enabling Syslog Accounting, page 3-11.

Tip With Cisco IOS Release 12.1(1)T, accounting based on SIP (Session Initiation Protocol) is provided through the command **gw-accounting voip**. To ensure that all relevant IOS versions are supported in networks where different IOS versions coexist, Cisco recommends that you cover all possible scenarios by entering the following commands— in the following order—on all GWs in your network:

```
gw-accounting voip
gw-accounting h323
gw-accounting h323 vsa
```

The above commands are discussed in greater detail in Configuring a Gateway for AAA, page 3-7.

Older Method: Enabling the Voice-Related CDR Field

In order to take advantage of standard RADIUS implementations that do not support vendor-specific attributes (VSAs), a method was defined that embedded the unsupported information elements in the RADIUS *Acct-Session-Id* field (RADIUS value 44 per RFC 2139). The *Acct-Session-Id* field has a maximum length of 256 bytes. It was defined to contain ten slash-separated fields, one of which is the RADIUS connection-id, which is a unique identifier that links accounting records associated with the same login session for a user. The internal representation of the *connection-id* field is 128 bits in hex format. This string can vary in appearance. In the examples cited in the CDR section of the *Configuration Guide for AAA Billing Features in Cisco Voice-Enabled Routers and Access Servers*, the *connection-id* is of the form 3C5AEAB9 95C80008 0 587F34 (one 4-octet string, a space, one 4-octet string, a space, a zero, a space, and one 3-octet string). The overloaded *Acct-Session-Id* field also contains connect and disconnect times, remote IP address, and disconnect cause.

In order to support these additional fields, the following string format for the Acct-Session-Id field is used:

```
<session id>/<call leg setup time>/<gateway id>/<connection id>/<call origin>/<call
type>/<connect time>/<disconnect time>/<disconnect cause>/<remote ip address>
```

This method is used with RADIUS call leg billing in a postpaid calling-card scenario, not in a prepaid scenario. The reason for this is that the GW does not receive an ACK from the RADIUS server.

Note For descriptions of the above, refer to Overloaded Acct-Session-Id Field Descriptions in *Configuration Guide for AAA Billing Features in Cisco Voice-Enabled Routers and Access Servers.*

To enable the gateway to recognize and use VSAs defined by attribute 26, use the **gw-accounting h323 vsa** command. After you enable VSAs, the *Acct-Session-Id* is no longer overloaded because the information sent in the session ID is captured in VSAs.

For more information on using VSAs with a RADIUS server, refer to the following:

RADIUS Vendor-Specific Attributes Voice Implementation Guide, Version 3.1, at

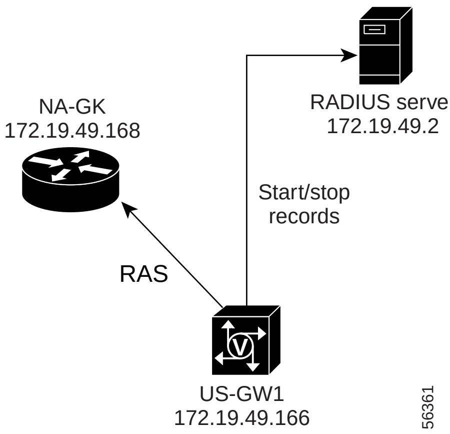
http://www.cisco.com/univercd/cc/td/doc/product/access/acs_serv/vapp_dev/vsaig3.htm

Configuring a Gateway for AAA

Figure 3-4 illustrates a subsection of GK zone NA-GK. The following example establishes AAA billing on US-GW1. There are three basic activities:

- Configure Communication between the Gateway and the RADIUS Server
- Configure the Gateway to Use VSAs
- Configure Gateway-Specific Accounting

Figure 3-4 Adding AAA Billing to a GW



Configure the following on all GWs that must communicate with a RADIUS server. Required and optional commands are so indicated.

Configure Communication between the Gateway and the RADIUS Server

First establish authenticated communication between the GW and the server. This allows the RADIUS server to recognize and use VSAs.

Note See AAA Accounting Commands, page 3-5. For details related to RADIUS implementations, refer to Configuring RADIUS at the following URL:
http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/secur_c/scprt2/scdrad.htm

Step 1 Enable AAA.

```
aaa new-model
```

Step 2 Configure the router to use the H.323 protocol list for authentication purposes.

```
aaa authentication login h323 group radius <---required; locks out Telnet session
aaa authentication login bypass none <---optional; use to prevent lockout
aaa authorization exec h323 group radius <---required
```

Following authentication, **exec** permits all necessary interactions.

Step 3 Define the accounting method list “h323” with RADIUS as a method. Here start-stop accounting will be used. The method list must be called *h323* and is activated for all voice interfaces—provided the **gw-accounting h323** command is also activated.

```
aaa accounting network h323 start-stop group radius <---optional
aaa accounting connection h323 start-stop group radius <---required
```

The command **connection** is critical.

Step 4 *[Optional]* Define a threshold time, in seconds, after which the router assumes that the RADIUS server is dead. After the threshold is exceeded, the router alerts an administrator that there is a security problem. Here we use 120 seconds (the default).

```
radius-server deadtime 120 <---optional
```

Step 5 Establish the IP address of the RADIUS server host, as well as the (well-known) ports for both the authentication and accounting services. The ports must match those of the RADIUS server.

```
radius-server host 172.19.49.2 auth-port 1645 acct-port 1646 <---port assignments required
```

Note The application listens for authorization on the *auth-port* and captures accounting data on the *acct-port*. The above port numbers are commonly used on Cisco GWs, but the actual ports referred to in the RADIUS protocol (and that are often used) are 1812 and 1813, for *auth-port* and *acct-port*, respectively. Again, the essential task is to match the port numbers with corresponding numbers on the RADIUS server.

Step 6 Configure the **radius-server** key secret. This establishes the shared secret text string that is used between the GW and the server. Here our *example* key is *lab.*

```
radius-server key lab
```

Step 7 *[Optional]* Specify the number of times (*retries*) the GW transmits each RADIUS request to the server before giving up. The default is three.

```
radius-server retransmit retries <---optional
```

Step 8 *[Optional]* Specify the number of seconds (*seconds*) the GW waits for a reply to a RADIUS request before retransmitting the request.

```
radius-server timeout seconds <---optional
```

Step 9 *[Optional]* Specify the number of minutes (*minutes*) that a RADIUS server failing to respond to authentication requests is passed over by requests for RADIUS authentication.

```
radius-server deadtime minutes <---optional
```

Step 10 Apply lockout prevention (see Step 2) to the vty ports:

```
line vty 0 4
password cisco
login authentication bypass
```

Configure the Gateway to Use VSAs

After communication is established, configure the GW to use vendor-specific RADIUS attributes.

Step 1 Enable VSA accounting.

```
radius-server vsa send accounting <---required
```

Step 2 Enable VSA authentication.

```
radius-server vsa send authentication <---required
```

Configure Gateway-Specific Accounting

Now use the command **gw-accounting** to establish H.323 accounting on the GW. Cisco recommends that you run the latest supported Cisco IOS software on all GWs. However, to cover all possible scenarios with a variety of IOS releases, Cisco recommends that you establish all three of the following options in the sequence below.

Note For the most current features, refer to *Enhancements to the Session Initiation Protocol for VoIP on Cisco Access Platforms*, at the following URL:
http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t3/dtsipgv2.htm

Step 1 Establish SIP accounting [IOS 12.1(1)T and later].

```
gw-accounting voip <---required
```

Step 2 Establish H.323 accounting.

```
gw-accounting h323 <---required
```

Step 3 Establish H.323 VSAs.

```
gw-accounting h323 vsa <---required
```

Note With Cisco IOS Release 12.1 an 11th field was added to the overloaded Acct-Session-ID list. This was to accommodate long-pound calls typical of card services.

Establishing Essential Files on the RADIUS Server

RADIUS applications vary, and are provided by a variety of vendors. Generally speaking, user keys and GW identities must reside in certain files in specified directories on the RADIUS server. This provides security for authentication. Check the installation instructions for your specific RADIUS application for the required locations and formats of these files.

However, to provide billing services, it is not sufficient to have only a standard RADIUS server. In order to support VoIP CDRs, billing partners must develop RADIUS applications that are customized to interact with Cisco GWs. Contact your Cisco account representative for developer support.

Using Network Time Protocol (NTP)

In order for the accounting records to include accurate connect and disconnect time records, Network Time Protocol (NTP) must be included in the router configuration. See Providing Network Timing through NTP, page 2-37.

For further information, including NTP time formats and links to useful sites, refer to Network Time Protocol (NTP) Usage Guidelines in *Configuration Guide for AAA Billing Features in Cisco Voice-Enabled Routers and Access Servers*, at the following URL:

http://www.cisco.com/warp/public/cc/so/cuso/sp/sms/acct/caaaf_cg.htm

Enabling Syslog Accounting

The Cisco IOS software can send syslog (system log) messages to one or more element management servers. Syslog messages are then collected by a standard UNIX or NT syslog daemon. These messages allow you to do the following:

- Centrally log and analyze configuration events and system error messages, such as interface status, security alerts, environmental conditions, and CPU process overloads.
- Capture client debug output sessions in real time.
- Reserve Telnet sessions for making configuration changes and using **show** commands, freeing the sessions from debug clutter.

The syslog accounting option exports the information elements associated with each call leg through a system log message that can be captured by a syslog daemon. The syslog output consists of the following:

```
<server timestamp> <gateway id> <message number> : <message label> : <list of A/V pairs>
```

Note This discussion is limited to RADIUS accounting (**gw-accounting h323**) only.

For information on enabling syslog, see Task 2. Enabling Syslog, at the following URL:

http://www.cisco.com/univercd/cc/td/doc/cisintwk/intsolns/as5xipmo/sysmgt.htm

Enabling SNMP

The SNMP (Simple Network Management Protocol) traps that are generated by Cisco routers provide useful information such as the following:

- Potentially harmful environmental conditions
- Processor status
- Port status
- Security issues

The Cisco IOS software generates SNMP traps depending on the features that the Cisco IOS release supports. For information on enabling SNMP, see Task 3. Enabling SNMP at the following URL:

http://www.cisco.com/univercd/cc/td/doc/cisintwk/intsolns/as5xipmo/sysmgt.htm

Caution Cisco recommends that you enable SNMP on all GWs. Otherwise, network management systems will not have access to the variables and trap information that they need as you use these applications. (It is the responsibility of the management application to process that information appropriately, and different applications support different SNMP features.) At the most basic level, simply set the SNMP enable community string parameter to **public**, and the management applications will take care of the rest.

Using a RADIUS MIB

You can also use a management information base (MIB) to manage RADIUS statistics on an AAA server. That SNMP version 2 MIB is located at the following URL:

ftp://ftp.cisco.com/pub/mibs/v2/CISCO-AAA-SERVER-MIB.my

For information about the MIB feature, refer to

Cisco AAA Server MIB and Additional Enhancements for the Cisco AS5300 and Cisco AS5800 Universal Access Servers, at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t3/dt_3asmb.htm

The above feature module discusses implementations of the Cisco AAA Server MIB to expand the RADIUS capabilities of the Cisco AS5300 series universal access servers.

For an example of these commands in configuration for a prepaid scenario, see Prepaid Card Services, page 3-15.

Tip To obtain lists of supported MIBs by platform and Cisco IOS release, and to download MIB modules, go to the Cisco MIB website on Cisco.com at the following URL: http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

Provisioning OSP Servers to the Gateway

In a VoIP environment involving multiple parties, the entity known as the clearinghouse is often the only way to handle call termination for the purpose of billing and settlement. Open Settlements Protocol (OSP) clearinghouses are third-party solutions that take advantage of OSP support in Cisco devices. This section discusses how to provision an OSP server to the GW.

Caution A special Cisco IOS image is required to support OSP. For the images required for each router type, see *Release Notes for the Cisco Wholesale Voice Solution*.

Note For more information about OSP, refer to “Open Settlements Protocol (OSP) Clearinghouse Solution,” Appendix A of the *Cisco Wholesale Voice Solution Overview.*

TransNexus

The TransNexus OSP Nexus™ Server provides carrier-grade clearinghouse interdomain authentication, routing (brokering), and CDR collection. Administered through a Web browser, the OSP Nexus Server provides centralized management of call routing, secure enrollment of network devices (such as GWs, GKs, call agents, and proxy servers), as well as easy integration with external billing and provisioning systems. More information about TransNexus products is available at http://www.transnexus.com.

Network devices query the server for call routing and authorization information, and report usage details to the server. Clearinghouse operators then collect from the server information related to rating, billing, and settlement.

Requirements

Recommended minimum hardware requirements are a Sun SPARCstation with a 300-MHz CPU and 512 MB of RAM. Solaris 7 or later is required.

Installation

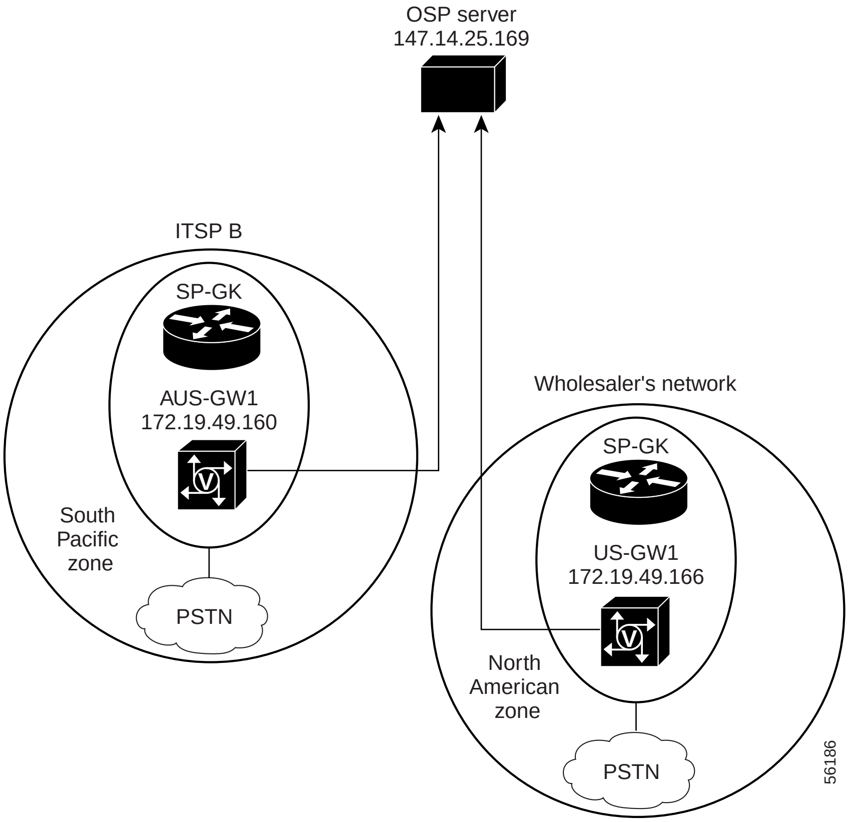
The installation and maintenance of this product are the responsibility of the service provider in conjunction with the product's representatives.

Configuring Gateways to Support OSP

Consider the following example. Figure 3-5 illustrates an OSP server that supports two independent zones, one belonging to a wholesale SP, the other to an ITSP. Billing software on the server is used to settle claims between the parties. Our example will look at the provisioning on the two GWs, AUS-GW1 and US-GW1.

Note Figure 2-17 on page 2-41 illustrates an example call flow for RAS failover to an OSP server.

Figure 3-5 An OSP Server Supporting Two Independent Zones



An analysis of the following configurations illustrates key provisioning and features.

AUS-GW1 Configuration

First look at AUS-GW1. Essentially the only items of interest in its configuration are the identity of the OSP server, the servers address, and the crypto certificates.

```
CRYPTO Certificate config

!
crypto ca identity DCL<----DCL is the identity of the OSP server
 enrollment url http://147.14.25.169:80/81 <---- protocol is http; OSP server’s address
 crl optional
crypto ca certificate chain DCL
 certificate 54 <---the crypto certificate follows
  30820206 3082016F A0030201 02020154 300D0609 2A864886 F70D0101 04050030
  2D310B30 09060355 04061302 5553310E 300C0603 55040A13 05436973 636F310E
  300C0603 55040313 056F7370 2D31301E 170D3031 30333032 32323439 30305A17
  0D303230 33303232 32343930 305A303E 310B3009 06035504 06130255 53310E30
  0C060355 040A1305 43697363 6F311F30 1D06092A 864886F7 0D010902 16107931
  2E666965 6C646C61 62732E63 6F6D305C 300D0609 2A864886 F70D0101 01050003
  4B003048 024100C3 82B4EAFD 1668C22C F1FF2609 35A63273 3D6BFC4E AE190BC3
  49DC990C 6DF497F4 1799FFB9 7BD519A9 DAC8870A 2F86CDDA DB05E861 2494FD46
  B8FB763B F026F102 03010001 A3693067 30090603 551D1304 02300030 0B060355
  1D0F0404 030205E0 304D0603 551D1F04 46304430 42A040A0 3E863C6C 6461703A
  2F2F6F73 702D312F 434E3D6F 73702D31 2C4F3D43 6973636F 2C433D55 533F6365
  72746966 69636174 65526576 6F636174 696F6E4C 69737430 0D06092A 864886F7
  0D010104 05000381 81003B8E 0E1809A3 76403529 FC02A523 EC8E0AFD 4A702EDB
  A9CCBBB8 5CB12984 B69D8A21 3E67A122 BDD86122 7131FE55 21CA2C94 3FA689C5
  52D29D31 542BB8B8 0BABD2D7 0AA054A3 5FE8A287 1DDE6504 B5D2A5FE C879BDFF
  1DE9294C 6FDC9F3C 5E35126E 200D9F19 F03589A8 F810FD17 221AC2E0 848E8BEA
  A03247A2 7EBA7185 289A
  quit
 certificate ca 01
  30820258 308201C1 A0030201 02020101 300D0609 2A864886 F70D0101 04050030
  2D310B30 09060355 04061302 5553310E 300C0603 55040A13 05436973 636F310E
  300C0603 55040313 056F7370 2D31301E 170D3030 30393330 30313432 33375A17
  0D313030 39333030 31343233 375A302D 310B3009 06035504 06130255 53310E30
  0C060355 040A1305 43697363 6F310E30 0C060355 04031305 6F73702D 3130819F
  300D0609 2A864886 F70D0101 01050003 818D0030 81890281 8100E009 863B2A53
  B21B7F23 D8F31F70 B2E1DF69 6FA0E7C3 851BCD08 78EEA950 BBD32EDF 21B42259
  7F5F31D0 B7C4EB29 A0D964C9 C0B1010E 26C202CB CE7B3E5D 8D932DD6 83EB0C32
  3AD1CAF6 1FC31BB6 8DFB2851 E2568956 9BF2AA49 F61FC3FF 29A2351E BC095B87
  022F4DDE FAB7A554 96C3A77C E42713EE 6CFBDE54 2CF8639C AC410203 010001A3
  81873081 84301D06 03551D0E 04160414 B44E41DE 7B1A3C7E 4C3E7171 74471C72
  6DAB4A57 30550603 551D2304 4E304C80 14B44E41 DE7B1A3C 7E4C3E71 7174471C
  726DAB4A 57A131A4 2F302D31 0B300906 03550406 13025553 310E300C 06035504
  0A130543 6973636F 310E300C 06035504 0313056F 73702D31 82010030 0C060355
  1D130405 30030101 FF300D06 092A8648 86F70D01 01040500 03818100 6A43ED0F
  0F9B5FBE 48DB09EE 3A6880FA 586D90F5 A848BB16 80257812 8FB7324B 6F74E3DC
  BC04D29E 8621B667 DBA6EB21 62603E6B FA827425 8AF1553D 6B720F25 C11334E2
  C19080AA 9F2BD742 AC01C892 471F8499 A6CE971C 59BDC184 41027F0C 878BAB36
  3B29D82B 99CA360B F6D33BCA DC756927 8FE59029 70016F52 77036408
  quit

<---snip--->

dial-peer voice 950 voip
 preference 5
destination-pattern 4085260
 session target settlement:0  <----the “settlement” statement
!
```

The settlement statement correlates the above destination pattern with the address of an OSP server.

```
settlement 0
```

```
type osp
url http://147.14.25.169<----address of OSP server
encryption des-cbc-sha
no shutdown
```

Tip For details of configuring settlement on third-party servers, refer to Configuring Settlement for Packet Telephony, at the following URL:
http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/multi_c/mcprt1/mcd4voip.htm

US-GW1 Configuration

The configuration of US-GW1 is essentially similar to the previous configuration.

Tip To avoid having to configure OSP on every GW, and to preserve the existing GK network, consider using back-to-back GWs, as discussed in Configuring Back-to-Back Gateways, page 2-44. For details, see Back-to-Back Gateway in an OSP Transit Zone, page 2-51.

Establishing Billing Systems for Calling Card Services

This section discusses the following:

- Prepaid Card Services
- Postpaid Card Services

In addition, the following commercial integrated billing applications are discussed briefly:

- MIND–iPhonEX Billing Support
- Clarent Clearinghouse Services

Note Where billing partners use the AMA (Automatic Messaging Accounting) format for billing records, the formatting of call-related data takes place at the billing server. Consequently, no special provisioning is required on the GWs with regard to the standard start/stop records that are sent. (In OSS, AMA is the automatic collecting, recording, and processing of call-related information for billing purposes.)

Prepaid Card Services

Figure 3-6 illustrates an example infrastructure required to support authorization and billing for prepaid calling card services.

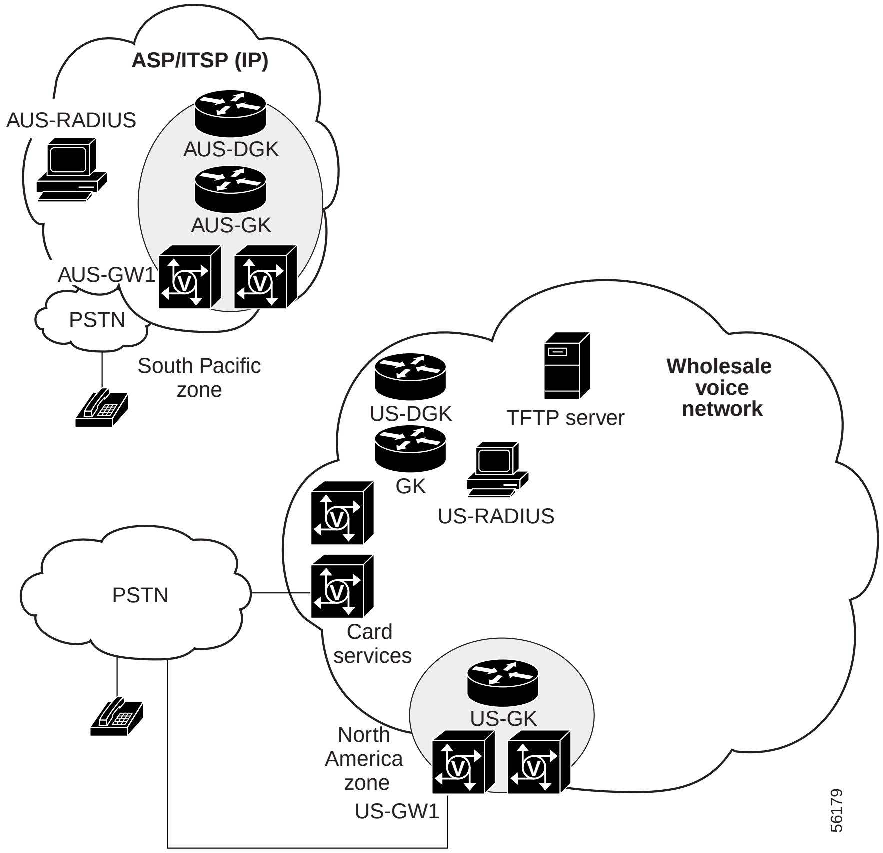
- Card services are delivered and billed at the GW.
- A TFTP server delivers audio prompt files to the GW.
- A RADIUS server (in this case MIND CTI) provides the AAA accounting application.

For details related to configuring prepaid and OSP-based services, refer to *Cisco Pre-Paid and OSP Configuration Guide*, at the following URL:

http://www.cisco.com/warp/public/cc/so/cuso/sp/prepd_cg.htm

For background on the required audio files and their support components, see Provisioning Services to Support IVR, page 3-19.

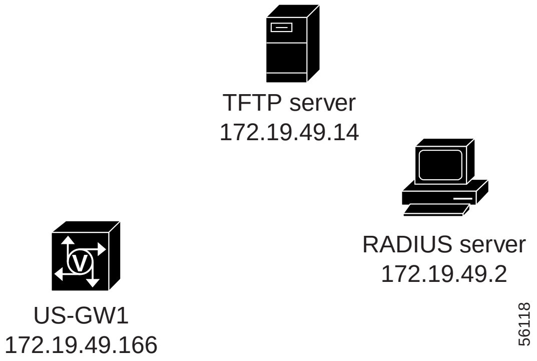
Figure 3-6 Authorization and Billing Infrastructure



Configuring a Gateway for Prepaid Card Service

Consider a simple example network consisting of a RADIUS server with IP address 172.19.49.2, a TFTP server with address 172.19.49.14, and a GW with address 172.19.49.166.

Figure 3-7 Example Network for Prepaid Calling Card Service



Apply the following example configuration to US-GW1 in global configuration mode. Refer also to the following:

- Understanding and Provisioning AAA Billing, page 3-2, and references therein.
- Configuring AAA Accounting, page 3-5

Note For useful background information and tips, refer to *Configuring Debit Card for Packet Telephony* at the following URL: http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/multi_c/mcprt1/mcd3voip.htm

However, the above document precedes TCL IVR 2.0, and some commands have since changed.

Step 1 Enable AAA.

```
aaa new-model
```

Step 2 Define an AAA RADIUS server.

```
aaa authentication login h323 group radius
aaa authentication login bypass none
aaa authorization exec h323 group radius
```

Step 3 Define the accounting method list "h323" with RADIUS as a method. Here start-stop accounting will be used. The method list must be called *h323* and is activated for all voice interfaces—if the **gw-accounting h323** command is also activated.

```
aaa accounting network h323 start-stop group radius
aaa accounting connection h323 start-stop group radius
```

Step 4 Assign a local reference name to the voice script for debit card (here arbitrarily called *debit*), and tell the GW where the TCL script is stored on the TFTP server.

```
call application voice debit tftp://172.19.49.14/tcl/debitcard.1.1.3.tcl
```

The system responds:

```
Loading tcl/debitcard.1.1.3.tcl from 172.19.49.14 (via Ethernet0/0): !!!!
[OK - 18387/35840 bytes]
Read script succeeded. size=18387, url=tftp://172.19.49.14/tcl/debitcard.1.1.3.tcl
```

Step 5 Establish parameters for the voice prompt. The next three line, respectively, refer to the file referenced as *debit* in Step 4.

a. Establish a length, in digits, for the user ID.

b. Establish an account-time remaining threshold, in seconds, at which a warning is activated.

c. Establish the language of the prompt message.

```
call application voice debit uid-len 6
call application voice debit warning-time 30
call application voice debit language 1 en
```

Step 6 Make sure to use the corresponding **set-location** command.

```
call application voice debit set-location en 0 tftp://172.19.49.14/prompts/en/
```

Step 7 Enable gw-accounting features.

```
gw-accounting h323
gw-accounting h323 vsa
```

```
gw-accounting voip
```

Step 8 Establish an IP address and ports for the RADIUS server.

```
radius-server host 172.19.49.2 auth-port 1645 acct-port 1646
radius-server retransmit 3
radius-server key testing123
radius-server vsa send accounting
radius-server vsa send authentication
```

Step 9 Configure the RADIUS server to be a slave to a master clock source (for example, 172.19.49.166). See Using Network Time Protocol (NTP), page 3-10.

```
ntp server 172.19.49.166
```

The router will now synchronize automatically with the master clock.

Postpaid Card Services

The provisioning required to support postpaid card services is essentially the same as that required for prepaid, with the exception that real-time interaction is not required. Although CDRs are still created, no real-time interaction with the user is required. The following activities, however, do take place:

- A VSA is required for debit and balance data.
- A query is sent to a database to authenticate the user's account.
- Another query is sent to a database to see if the dial plan is part of a billing system.

However, the above are all read-only activities: no records need to be updated until the call is completed.

MIND–iPhonEX Billing Support

MIND-iPhonEX is a web-based VoIP billing solution provided by MIND CTI. This integrated product performs caller authentication, authorization, and accounting in real time, and provides for the creation and management of prepaid calling cards, real-time call rating, and billing of credit customers. For more information about MIND CTI and their products, visit http://www.mindcti.com.

Caution MIND-iPhonEX does not support the use of the md5 hashed password. The md5 hashed password is required for H.235 security.

Requirements

In order to accommodate large numbers of customer accounts, MIND offers a UNIX real-time server (RTS). Multiple RTSs can be installed to provide load sharing and failover functionality, as required. In addition, to provide reliability and scalability, MIND -iPhonEX uses an Oracle database. Contact your MIND representative for the most current requirements, both hardware and software, of the RTS and database.

Installation

Cisco is not responsible for installing, provisioning, or maintaining MIND CTI's products.

Clarent Clearinghouse Services

Clarent Command Center can be used as part of the Cisco Wholesale Voice Solution to provide centralized billing, network management of user accounts, dynamic call routing, flexible call rating, and subscriber authentication. A centralized database provides a single point of administration for distributed networks. For more information about Clarent and their products, visit http://www.clarent.com

Among other features, Clarent Command Center provides the following billing options:

- Call Detail Records—Track telephone calls. The service code includes five types of billing records: voice, fax, data, administration, and CDR. This option can collect billing and nonbilling records.
- Flexible Call Rating—Allows either point-to-point billing or flat-rate billing call rating. The SP can rate calls on a countrywide basis or can be more precise and bill calls on a city-by-city basis. Calls are distinguished between internal, external, and calling card calls made from sites outside the SP's own network. Different inbound and outbound charges can be set for each route.
- Billing Options—Support debit cards and standard open-account billing. Accounts can be grouped to track sales or announce special messages and new features.
- Real-time Billing—Prevents duplicate simultaneous account usage, reducing fraudulent calls made outside of the Command Center or from a prepaid calling card.

Requirements

Clarent recommends that Clarent Command Center run on a dedicated NT server with a Pentium II processor (minimum 366 MHz) with at least 128 MB of RAM and a 4.3 GB hard drive. For current information and complete details, refer to *Clarent Command Center Technical Reference, Release 3.1* or later, or contact a Clarent representative.

Installation

Cisco is not responsible for the installing, provisioning, or maintaining Clarent's products. Refer to *Clarent™ Command Center Technical Reference, Release 3.1* or later for currrent information (including complete hardware and software requirements) on how to install, configure, and operate Clarent Command Center.

Provisioning Services to Support IVR

To support services that require interactive voice messaging, such as for a prepaid card service that requests a user's PIN number and notifies the user of the number of minutes remaining, several components require consideration.

- A TFTP (Trivial File Transfer Protocol) server will be needed to host the TCL (Tool Control Language) scripts and audio files.
- Cisco TCL IVR (Interactive Voice Response) scripts will be required to gather information and process accounting and billing data.
- TCL scripts may be needed to tailor or develop the required scripts for a specific application. Scripts can be easily modified to add custom features.

These issues are discussed, respectively, in the following sections:

- TFTP Servers, below
- Cisco TCL IVR, page 3-22

TFTP Servers

TFTP, a connectionless protocol based on UDP, is inherent in most UNIX systems. TFTP is used to transfer files between remote file systems and GWs with a minimum of interactive overhead—and security (thus the term "trivial"). In addition to hosting and delivering Cisco IOS images, a TFTP server has a significant role to play in a wholesaler's network where interactive voice prompts, often in multiple languages, are required. This section addresses the use of a TFTP server to host audio files.

You must begin by ensuring that the TFTP daemon is enabled and a *tftpboot* directory exists. Follow the steps below to enable TFTP on the server.

Enabling the TFTP Daemon

In order to upload or download a configuration file, the TFTP daemon (*tftpd*) must be enabled. If you are using the standard Sun software, verify that *tftpd* is enabled by completing the following steps:

Step 1 Log in as a super user.

Step 2 Using a text editor such as vi, edit the file */etc/inetd.conf* file.

Step 3 Look in the file */etc/inetd.conf* for the line that invokes *tftpd*. If the line is commented out [starts with a pound (#) as in the following example],

```
#tftp dgram udp wait root /user/etc/in.tftpd in.tftpd -s /tftpboot
```

Use the text editor to remove the pound (#) sign so that only the following remains:

```
tftp dgram udp wait root /user/etc/in.tftpd in.tftpd -s /tftpboot
```

Note The argument -*s* indicates that this is a Solaris system.

Step 4 Save the changes in the edited file and exit.

Step 5 At the UNIX prompt, enter the following command to display the process id number for the *inetd* configuration.

```
hostname# ps -ax | grep -v grep | grep inetd
```

The system responds with something similar to the following:

```
hostname# 119 ? S 0:05 inetd
```

The first number in the output is the process ID of the *inetd* process (in the above example, 119).

Step 6 You must restart the process by entering the following:

```
kill -HUP <your process number>
```

Step 7 Verify that TFTP is enabled by typing the following:

```
netstat -a | grep tftp
```

The output should be similar to the following:

```
*.tftp Idle
```

If there is no output, *tftpd* is not enabled.

Note For additional information on TFTP, refer to the UNIX man pages on *tftp* and *tftpd*.

Creating the *tftpboot* Directory

The *tftpboot* directory can be used to save and store voice and configuration files that are loaded to a GW. By default, the *tftpboot* directory resides at the root of the host server file system. This ensures that a requesting system can find the directory easily and consistently. Look at the root directory to see if *tftpboot* exists. If it does not, follow the steps below to create the directory.

Step 1 Use the following command at the UNIX prompt to create the *tftpboot* directory:

```
mkdir /tftpboot
```

Step 2 The *tftpboot* directory must have the appropriate permissions. To ensure the correct permissions, modify them with the following command:

```
chmod 777 /tftpboot
```

As a result, all users accessing the *tftpboot* directory will have read, write, and execute permissions.

Enabling TFTP on the GWs to Support Call Application Functions

The following illustrates how to enable the downloading of voice prompt files to a GW. You will need to enable TFTP access on each GW to which files are to be downloaded. This includes telling the GW the IP address of the machine on which the files are stored. Enter the privileged EXEC mode on the access router to enable the following steps.

Step 1 Create a name for the file. Replace *my_debit_file* with a name of your choice. Then assign a TFTP IP address for the TFTP server, and indicate the directory in which the file resides.

```
Router(config)# call application voice my_debit_file
tftp://172.19.49.14/tcl/debitcard.1.1.3.tcl
```

Note For the above and following command, refer to the *Cisco IOS Multiservice Command Reference* for a discussion of **call application voice**.
Refer to
http://www/univercd/cc/td/doc/product/software/ios121/121cgcr/multi_r/mrd_a.htm
and especially to
http://www/univercd/cc/td/doc/product/software/ios121/121cgcr/multi_r/mrd_a.htm#1023041

Step 2 Use the parameter **uid-len** to define the number of characters in the UID (user ID) for the designated application. This also passes that information to the call application.

```
Router(config)# call application voice debit uid-len 6
```

Note The default value for **uid-len** is 10. The parameter **pin-len** (Personal ID Number length) is also available, with a default value of 4.

Step 3 Use the parameter **warning-time** to define the number of seconds that a user is told to remain before the user's allows calling time runs out for a designated application. The following example shows a warning time of 30 seconds.

```
Router(config)# call application voice debit warning-time 30
```

Step 4 Determine the language of the audio file. Valid entries are **en** (English), **sp** (Spanish), **ch** (Mandarin), and **aa** (all).

```
Router(config)# call application voice debit language 1 en
```

Note The number following language is arbitrary. For example, to assign Spanish as a second language, you could enter `language 2 sp`.

Step 5 Determine the location, language, and category of the audio files for the designated call application, and pass that information to the application.

```
Router(config)# call application voice debit set-location en 0
tftp://172.19.49.14/prompts/en/
```

Cisco TCL IVR

Interactive Voice Response (IVR) consists of simple voice prompting and digit collection to gather caller information for authenticating the user and identifying the destination. IVR applications can be assigned to specific ports or invoked based on DNIS. An IP PSTN gateway can have several different IVR applications to accommodate many different gateway services, and you can customize the IVR applications to present different interfaces to the different callers.

IVR uses Tool Control Language (TCL) scripts to gather information and to process accounting and billing. (When used together in Cisco applications, Cisco refers to the combination as Cisco TCL IVR.) For example, a Cisco TCL IVR script plays when a caller receives a voice-prompt instruction to enter a specific type of information, such as a PIN. After playing the voice prompt, the IVR application collects the predetermined number of touch tones (digit collection) and forwards the collected digits to a server for storage and retrieval. Call records can be kept and a variety of accounting functions performed.

Cisco provides a variety of scripts, among them the following:

- *fax_hop_on_1*—Collects digits from the redialer, such as account number and destination number. When a call is placed to an H.323 network, the set of fields configured in the call information structure are *entered*, *destination*, and *account*.
- *clid_authen*—Authenticates the call with ANI and DNIS numbers, collects the destination data, and makes the call.
- *clid_authen_npw*—Same as *clid_authen*, but uses a null password when authenticating, rather than DNIS numbers.
- *clid_authen_collect*—Authenticates the call with ANI and DNIS numbers and collects the destination data, but if authentication fails, it collects the account and password.

- *clid_authen_col_npw*—Same as *clid_authen_collect*, but uses a null password and does not use or collect DNIS numbers.
- *clid_col_npw_3*—Same as *clid_authen_col_npw*, except that with that script, if authentication with the digits collected (account and PIN) fails, the *clid_authen_col_npw* script just plays a failure message (*auth_failed.au*) and then hangs up. The *clid_col_npw_3* script allows two failures, then plays the retry audio file (*auth_retry.au*) and collects the account and PIN again.

Note To see all available scripts on a GW, enter the command **show call application voice summary**.

The caller can interrupt the message by entering digits for the account number, which triggers the prompt to tell the caller to enter the PIN. If authentication fails the third time, the script plays the audio file *auth_fail_final.au*, and hangs up.

For more information about IVR, refer to the following documents at their respective URLS:

- *Configuring Interactive Voice Response*, at

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/multi_c/mcprt1/mcd2voip.htm

- *Configuring Interactive Voice Response for Cisco Access Platforms*, at

http://www.cisco.com/univercd/cc/td/doc/product/access/acs_serv/5300/sw_conf/ios_121/0061ivr.htm

- *TCL IVR API Version 2.0 Programmer's Guide*, at

http://www.cisco.com/univercd/cc/td/doc/product/access/acs_serv/vapp_dev/tclivrv2.htm

- *VoIP with IVR*, at

http://www.cisco.com/warp/public/788/voip/voip_gw_ivr2.htm

TCL is an open-standard interpreted scripting language. (Version 8 is the most recent release.) Because TCL is an interpreted language, scripts written in TCL do not have to be compiled before they are executed. TCL provides a fundamental command set, which allows for standard functions such as flow control (*if*, *then*, *else*) and variable management. By design, this command set can be expanded by adding extensions to the language to perform specific operations.

Cisco has created a set of extensions, called TCL IVR commands, that allows users to create IVR scripts using TCL. Unlike other TCL scripts, which are invoked from a shell, TCL IVR scripts are invoked when a VoIP call comes into the gateway.

For more information about TCL and how to use the API to write new scripts, refer to the following document:

- TCL IVR API Version 2.0 Programmer's Guide, at

http://www.cisco.com/univercd/cc/td/doc/product/access/acs_serv/vapp_dev/tclivrv2.htm

Using Network Management Applications

It is one thing to consider provisioning and maintenance in the abstract, and quite another to implement provisioning and maintenance throughout a large network. Success and cost-effectiveness in large networks requires management, performance monitoring, and maintenance applications, of which a variety are discussed below. The following are discussed in this section:

- Element Management Systems
- Performance and Statistical Reporting Tools
- Installing Network Management Applications

Element Management Systems

CiscoWorks2000 Voice Manager

CiscoWorks2000 Voice Manager (CVM) version 2.0.2 (see CiscoWorks2000 Voice Manager, page 3-24) is an element management system that provides the following features:

- Support for basic VoIP configuration parameters, such as interface signaling types, dial peers, and H.323 registrations
- Simple dial-plan provisioning (within a local region only)
- Support for SNMP MIB management of any SNMP-capable device

For information about CiscoWorks2000, see About CiscoWorks2000, below. To install CiscoWorks2000 Voice Manager, see Installing CiscoWorks2000 Voice Manager, page 3-28.

About CiscoWorks2000

CiscoWorks2000 is a family of products that provide solutions targeted at WAN and LAN operations of enterprise networks. CVM and Cisco Info Center (CIC) (see Cisco Info Center, page 3-26) are members of this family. For details see CiscoWorks2000 at the following URL:

http://www.cisco.com/warp/public/44/jump/ciscoworks.shtml

Performance and Statistical Reporting Tools

A critical part of a service provider’s operations support system (OSS) is performance and statistical reporting. (Other critical OSS components include billing, provisioning, fault management, and real-time monitoring.) Performance reporting facilitates the following important functions:

- Historical performance monitoring and trending, including QoS
- Capacity planning
- Troubleshooting

The following applications are discussed in this section:

- CiscoWorks2000 Voice Manager
- Cisco Info Center
- Cisco Internet Performance Manager
- Trinagy Voice Over IP ReportPack 1.1

CiscoWorks2000 Voice Manager

Overview

CiscoWorks2000 Voice Manager (CVM) Release 2.0.2 is the application of choice for supporting performance and statistical reporting for the Cisco Wholesale Voice Solution. CVM is a client/server, web-based solution to managing the VoIP functionality of the Cisco 3600 series routers used in the solution. CVM allows you to do the following:

- Configure dial plans and voice interfaces

- Monitor SNMP traps and resource utilization
- Test dial-path configurations and connectivity
- Generate call history reports

Note CVM version 2.0.2 is *required*.

With respect to network performance, CVM provides the following reporting features:

- An open interface enabling third-party management systems to gather and correlate data
- Polling of GWs for call history statistics
- A clean, well-formatted VoIP call-history file, allowing third-party applications to obscure platform statistics
- Reporting data for use in troubleshooting and traffic forecasting
- Reports, including answer seizure rate, call success rate, call volumes, and disconnect causes
- Support for scalability through the modeling of hierarchical GK design (CVM resources can be inserted on demand as capacity and network coverage area grow)

SNMP Foundation

CVM is not a device configuration tool. Devices supported by CVM must first be configured through the command-line interface (CLI) and have Simple Network Management Protocol (SNMP) enabled before they can be managed by CVM. (See Enabling SNMP, page 3-11.) You can then use CVM to modify the configuration of voice ports and create and manage local and network dial plans.

For additional information about SNMP, refer to the following:

- Simple Network Management Protocol (SNMP), at

  http://www.cisco.com/cpress/cc/td/cpress/fund/ith2nd/it2452.htm
- Enabling Management Protocols: NTP, SNMP, and Syslog, at

  http://www.cisco.com/univercd/cc/td/doc/cisintwk/intsolns/as5xipmo/sysmgt.htm

CVM's support for SNMP includes trap viewing and forwarding. CVM 2.0.2 can receive and collect traps from GWs through SNMP. Traps can be forwarded to Cisco Info Center (CIC) for event correlation.

Note CVM is a stand-alone product that is not appropriate to the scaling needs of large-scale service providers. Although CVM can be used on a POP basis for small to medium service providers, it is not suitable for wholesale providers. It is used primarily with a polling application. In order to provide an effective distributed reporting solution, CVM requires integration with a third-party partner.

Requirements and Installation

See Installing CiscoWorks2000 Voice Manager, page 3-28.

Cisco Info Center

Overview

Cisco Info Center (CIC) is another member of the CiscoWorks2000 family. CIC provides the following features with respect to fault management and event correlation:

- Optimizes fault management by reducing alarm information overload through “de-duplication” and fault correlation; this enables faster problem solving and better operations scaling.
- Flexibly manages and monitors faults in multivendor, multitechnology, and multiservice environments.
- Correlates faults received from multiple sources, such as SNMP traps and syslog events.
- Supports distributed operational environments, to do such things as the following:
  - Reduce the number of NOCs (network operations centers).
  - Provide centralized and regional monitoring.
  - Eliminate costly, inefficient “console farms” of scrolling alarms.
- Can translate faults and events into actions, to do such things as the following:
  - Page key maintenance personnel.
  - Issue trouble tickets.
  - Send alarms for critical events.
- Provides a distributed, redundant architecture, for scaling and reliability.

The most current version is Release 2.0. For additional information, see *Cisco Info Center 2.0 Release* at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/info_ctr/2_0_0/index.htm

Requirements and Installation

See Installing Cisco Info Center, page 3-31.

Cisco Internet Performance Manager

Overview

Cisco Internet Performance Manager (IPM) is a performance management application that can monitor the performance of a service provider’s network. Cisco IPM provides the following features related to network performance:

- Provides real-time and historical network-performance reports on VoIP characteristics such as the following:
  - Latency
  - Jitter
  - Packet errors
  - Packet loss for all available IP paths
- Measures network performance on a hop-by-hop basis, to do such things as the following:
  - Pinpoint latency and jitter causes.

  - Reduce problem isolation and resolution time.
- Generates traps based on response-time thresholds, to provide real-time alerting of potential problems.
- Works with Cisco IOS Service Assurance Agent (SAA) to support service level measurement.

The most current version of Cisco IPM is Release 2.3. Release notes, an installation guide, a user guide, and FAQs are available at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/ipmcw2k/cipm23/index.htm

Overviews, data sheets, product bulletins, and an IP tutorial are available at the following URL:

http://www.cisco.com/warp/public/cc/pd/wr2k/nemo/prodlit/index.shtml

For information about SAA, refer to Network Monitoring Using Cisco Service Assurance Agent, at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/fun_c/fcprt3/fcd301d.htm

Requirements and Installation

To install the latest version, see Installing Cisco Internet Performance Manager, page 3-31.

Trinagy Voice Over IP ReportPack 1.1

Overview

Cisco and Ecosystem Partner Trinagy, Inc. (http://www.trinagy.com) have collaborated to develop a new performance reporting tool for H.323-based VoIP networks. The product, called Voice Over IP ReportPack v. 1.1, provides seven reports that focus on GW devices and groups of GW devices. The groups are typically named Gateway, Gateway Group, Customer, and Region, but the user can customize the names and grouping structure. Each of the seven reports can be applied to the four groupings of data, for a total of 28 reports. The seven reports types are as follows:

- QoS hot spots
- Call minutes
- Call success rate
- Call volume
- Disconnect cause
- International v. domestic
- Minutes of use (for all devices used in the previous 24-hour period)

Each report contains a selection table with the names of network devices or groups of network devices, with columns of data displayed in table format. Tabular data can also be displayed graphically, with more detail about a selected GW.

Requirements and Installation

See Installing Trinagy Voice Over IP ReportPack 1.1, page 3-32.

Installing Network Management Applications

Installing CiscoWorks2000 Voice Manager

Understanding Prerequisites

Step 1 Refer to the following website:

CiscoWorks2000 Voice Manager 2.0.2, at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/voicemgr/cvm2x/cvm202/index.htm

Note The following steps refer to documents at the above URL. The information provided there is applicable to version 2.0.2. However, in the discussion that follows, the application is referred to generically as CVM 2.0.

Step 2 Refer to the following online document at the *CiscoWorks2000 Voice Manager 2.0* website: *CiscoWorks2000 Voice Manager 2.0 Installation and User Guide*.

Step 3 Refer to the following chapter in the above document: "Overview of CiscoWorks2000 Voice Manager 2.0"

Step 4 Refer to the section "Planning for CVM," and understand the subsection Prerequisites. Before you can use CVM to manage your voice network, you will need to do the following for all of the devices you want to manage:

a. Have network access to the devices.

b. Enable Telnet on all the devices.

c. Enable SNMP on all the devices.

d. Ensure that GKs to be added to CVM are running the appropriate Cisco IOS release.

e. Know the IP address of the devices.

f. Know the passwords of the devices.

g. Know the SNMP read community string for the devices.

Step 5 Proceed to the following section, Determining Requirements.

Determining Requirements

Step 1 Refer to the following online document at the *CiscoWorks2000 Voice Manager 2.0* site: *CiscoWorks2000 Voice Manager 2.0 Installation and User Guide*.

Step 2 Refer to the following chapter in the above document: "Installing CiscoWorks2000 Voice Manager 2.0"

Step 3 Determine your platform. CVM supports two platforms: Windows NT and Solaris.

Step 4 Refer to the section "System Requirements" in the document you selected in Step 2. Note the requirements for your platform and make sure you meet those requirements.

Caution Service Pack 5 is required for Windows NT installations.

Note Unless otherwise noted, requirements are minimum requirements, but may be entirely satisfactory.

Step 5 Proceed to the following section, Installing CVM.

Installing CVM

Step 1 Refer to the following online document at the *CiscoWorks2000 Voice Manager 2.0* site:
CiscoWorks2000 Voice Manager 2.0 Installation and User Guide.

Step 2 Refer to the following chapter in the above document:
"Installing CiscoWorks2000 Voice Manager 2.0"

Step 3 Follow the instructions in the above chapter to install the necessary software from your CVM installation CD.

Step 4 For background, read the remainder of the chapter you selected in Step 2.

Step 5 Proceed to the following section, Starting CVM.

Starting CVM

Step 1 Refer to the following online document at the *CiscoWorks2000 Voice Manager 2.0* site:
CiscoWorks2000 Voice Manager 2.0 Installation and User Guide.

Step 2 Refer to the following chapter in the above document:
"Getting Started with CiscoWorks2000 Voice Manager 2.0"

Step 3 Refer to the section "Starting CVM" in the above chapter, and follow the instructions there.

Step 4 You will now need to configure CVM to poll. Proceed to the following section, Configuring CVM to Poll.

Configuring CVM to Poll

Step 1 Refer to the following online document at the *CiscoWorks2000 Voice Manager 2.0* site:
CiscoWorks2000 Voice Manager 2.0 Installation and User Guide.

Step 2 Refer to the following chapter in the above document:
"Getting Started with CiscoWorks2000 Voice Manager 2.0"

Step 3 Refer to the section User Interface in the above chapter, and learn about Views and Device Trees.

Note You will need to select VoIP View to see VoIP-enabled devices that have been added to CVM. You will not need to create a group, because groups are required only for VoIP networks whose routers are not managed by a gatekeeper

Step 4 Select VoIP View.

Step 5 Use drag-and-drop to add the GWs and GKs in your configuration to the selected view.

Adding Gateways

Adding GWs is similar to adding routers. You will first need to enable Telnet and SNMP, and configure the session timeout to a nonzero value for all vty lines.

Step 1 Refer to the following online document at the *CiscoWorks2000 Voice Manager 2.0* site:
CiscoWorks2000 Voice Manager 2.0 Installation and User Guide.

Step 2 Refer to the following chapter in the above document:
"Using CiscoWorks2000 Voice Manager 2.0 to Manage Devices"

Step 3 Refer to the section "Routers" in the above chapter, and follow the commands listed there to do the following:

- **a.** Enable SNMP.
- **b.** Configure *enable* or *secret* password.
- **c.** Create line password to enable Telnet.
- **d.** Configure a session timeout for all vty lines.

Note CVM searches the GWs and automatically detects the type of voice interfaces enabled on them, placing the devices in the appropriate view. The GWs will appear in the All Router view as well.

Adding Gateways to Gatekeepers

Step 1 Refer to the following online document at the *CiscoWorks2000 Voice Manager 2.0* site:
CiscoWorks2000 Voice Manager 2.0 Installation and User Guide.

Step 2 Refer to the following chapter in the above document:
"Using CiscoWorks2000 Voice Manager 2.0 to Manage Devices"

Note The following references to routers apply to GWs.

Step 3 Refer to the section "Routers" in the above chapter, and follow the commands listed there to do the following:

- **a.** Select the GK to which you wish to add the GW.
- **b.** Enter the following values for the GW: IP address, (SNMP) community string read, community string write.
- **c.** Enter the following values for the terminal server on which CVM resides: IP address, port, login username.
- **d.** Enter the following passwords for the GW: login, enable, secret.

Step 4 To accomplish the above, follow Steps 1 through 5 under the section "Adding a Router."

Step 5 Continue with Steps 6 through 10 in the above section, to finish adding the device to the Device Tree Hierarchy.

Step 6 For each device that you want to add, repeat Steps 1 through 10 under the section “Adding a Router.”

Managing Dial Plans

You can use CVM to manage dial plans, as shown in the following steps.

Step 1 Refer to the following online document at the *CiscoWorks2000 Voice Manager 2.0* site: *CiscoWorks2000 Voice Manager 2.0 Installation and User Guide*.

Step 2 Refer to the following chapter in the above document:
“Using CiscoWorks2000 Voice Manager 2.0 to Manage Dial Plans”

Step 3 Become familiar with the information in the above chapter. You can create and modify both local (POTS) and network (VoIP) dial plans.

Installing Cisco Info Center

This discussion concerns the latest release of Cisco Info Center, Release 3.0.1. Information about all CIC releases is available at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/info_ctr/

For requirements and installation, refer to *Release Notes for Cisco Info Center 3.0.1*, at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/info_ctr/3_0_1/notes301.htm

Requirements

Refer to “Supported Hardware and Software” in the above document.

Installation

Refer to “CIC 3.0.1 Installation Instructions” in the above document.

Installing Cisco Internet Performance Manager

The latest version is Release 2.3. (See Cisco Internet Performance Manager, page 3-26.) The following discussion relates to Internetwork Performance Monitor, Release 2.3, at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/ipmcw2k/cipm23/ipm23ig/index.htm

Requirements

Read “Preparing to Install IPM, “at the above website. Instructions are also provided for upgrading from previous releases of Cisco IPM.

Installation

Cisco IPM runs on Solaris and Windows platforms. Depending on your platform, see either "Installing IPM on Solaris" or "Installing the IPM Client on Window"s at the above website.

Installing Trinagy Voice Over IP ReportPack 1.1

Requirements

The application runs on a UNIX workstation and requires two other Trinagy applications: Trinagy TREND 3.6.1 or later, and Trinagy TRENDweb 3.2. In addition, Perl 5.6 or later must be installed before Voice Over IP ReportPack v. 1.1 is installed. Perl creates the necessary directory structure, and can be downloaded from http://www.perl.com.

Note Contact your Trinagy representative or Cisco account representative for the most current hardware and software requirements.

Installation

The acquisition and installation of this reporting tool are beyond the scope of this document. Trinagy provides their own documentation to install and use TREND and the ReportPack application. For further information, please contact your Trinagy representative or Cisco account representative.

CHAPTER 4

Provisioning Non-SS7-Based POPs

Introduction

Provisioning for POPs that do not require SS7 signaling is relatively simple. The fundamentals of installing the interface hardware have already been covered in Chapter 2, "Provisioning the Gatekeeper Core." Refer in particular to Establishing Gateways, page 2-59, taking care to select the appropriate Cisco hardware. Table 2-4 on page 2-59 discusses the interface cards and signaling types they support.

This chapter presents the following major topics:

- Provisioning References
- Configuration Examples

Caution Always consult with your telecommunications service provider to determine the appropriate signaling parameters for your Cisco interfaces. Before configuring ISDN PRI on your Cisco router, you need to order a correctly provisioned ISDN PRI line from your telecommunications service provider.

Provisioning References

For background, references for provisioning signaling and other fundamentals are provided below for the Cisco routers that are used as GWs, as well as for the latest version of the Cisco IOS.

Tip Information related to provisioning a particular Cisco voice GW may be obsoleted by the most current release of Cisco IOS software.

For Routers

The following provides links to online provisioning references for the following GW types:

- Cisco 3600 Series
- Cisco AS5300
- Cisco AS5350 and Cisco AS5400

Cisco 3600 Series

To provision Cisco 3600 series GWs, refer to the following for these routers:

Software Configuration Guide

at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/access/acs_mod/cis2600/sw_conf/26_swcg/index.htm

In particular, see "Configuring with the Command-Line Interface," at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/access/acs_mod/cis2600/sw_conf/26_swcg/config.htm

The following topics are of interest here:

- Configuring ISDN BRI WAN Interfaces
- Configuring T1 and E1 Interface Cards

Cisco AS5300

To provision Cisco AS5300 GWs, refer to the following for these routers:

Cisco AS5300 Software Configuration Guide

at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/access/acs_serv/5300/sw_conf/sw_conf/index.htm

In particular, see "Basic Configuration," at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/access/acs_serv/5300/sw_conf/sw_conf/5300bas2.htm

The following topics are of interest here:

- Configuring Channelized T1 or E1
- Configuring ISDN PRI
- Configuring E1 R2 Signaling

Cisco AS5350 and Cisco AS5400

To provision Cisco AS5350 and Cisco AS5400 GWs, refer to the following document for these routers:

Cisco AS5350 and Cisco AS5400 Universal Gateway Software Configuration Guide

at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/access/acs_serv/as5400/sw_conf/53swcg/index.htm

In particular, see "Basic Configuration Using the Command Line Interface (CLI)," at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/access/acs_serv/as5350/sw_conf/53swcg/54bas2.htm

The following topics are of interest here:

- Configuring Channelized T1 and E1 Dial Feature Cards
- Configuring ISDN PRI
- Configuring the D Channels for ISDN Signaling

Configuration Examples

Configuration specifics are provided later in this section for the following basic signaling types:

- E1 R2
- PRI ETSI
- PRI NI2
- T1 CAS FGB
- T1 CAS FGD

The basic configurations are as provided in Configuring Gateway Interfaces to the PSTN, page 2-12.

Note As of the time of this writing, documentation for Cisco IOS 12.2 is the most recent. Documentation for Release 12.2 is available at the following URL:
http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/index.htm

For a practical background to the following discussion, refer to Configuring ISDN PRI and Other Signaling on E1 and T1 Lines, at the following URL:
http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/dialts_c/dtsprt3/dcdchant.htm

Configuration Fundamentals: Configuring T1 Signaling on a Cisco AS5300

The following is an example basic configuration of a T1 interface on a Cisco AS5300. The following steps do only the following:

1. define a T1 controller interface
2. Assign a DS0 group number to the T1 interface
3. Assign T1 timeslots (DS0 channels) to the T1 interface
4. Assign the signaling type to the T1 interface

Step 1 Enter terminal configuration mode and assign a controller ID for one T1 interface.

```
wz7-5300-2# conf t
Enter configuration commands, one per line.  End with CNTL/Z.
wz7-5300-2(config)# controller t1 0
```

Step 2 Assign a DS0 group that represents the T1 interface. Here we choose 0.

```
wz7-5300-2(config-controller)# ds0-group ?
  <0-23>  Group Number

wz7-5300-2(config-controller)# ds0-group 0 ?
  timeslots  List of timeslots in the ds0-group
```

Step 3 Assign DS0 channels 0 through 23 to the interface.

```
wz7-5300-2(config-controller)# ds0-group 0 time ?
  <1-24>  List of T1 timeslots

wz7-5300-2(config-controller)# ds0-group 0 time 1-24 ?
  service  Specify the type of service
  type     Specify the type of signaling
  <cr>
```

Step 4 Assign a signaling type to the DS0 channels (collectively). Note the options.

```
wz7-5300-2(config-controller)# ds0-group 0 time 1-24 type ?
  e&m-fgb              E & M Type II FGB
  e&m-fgd              E & M Type II FGD
  e&m-immediate-start  E & M Immediate Start
  fgd-eana             FGD Exchange Access North American
  fgd-os               FGD Operator Services
  fxs-ground-start     FXS Ground Start
  fxs-loop-start       FXS Loop Start
  none                 Null Signalling for External Call Control
  r1-itu               R1 ITU
  sas-ground-start     SAS Ground Start
  sas-loop-start       SAS Loop Start
  <cr>
```

Here we choose E&M Feature Group B (wink start protocol), and choose MF (multifrequency) signal tones.

```
wz7-5300-2(config-controller)# ds0-group 0 time 1-24 type e&m-fgb mf
```

Note For other provisioning features and related information, refer to the documentation for provisioning this series of routers, in the references above.

Signaling Types and Examples

The following examples (presented in alphabetical order) illustrate the key parameters required for the various signaling types.

E1 R2

```
controller E1 1
 clock source line primary
 ds0-group 1 timeslots 1-15,17-31 type r2-digital
 cas-custom 1

voice-port 1:1

interface Serial0:15
 no ip address
 no ip directed-broadcast
 isdn switch-type primary-ni
 fair-queue 64 256 0
 no cdp enable
```

PRI ETSI

```
controller E1 0
 pri-group timeslots 1-31

voice-port 0:D
```

PRI NI2

```
controller T1 2
 framing esf
 clock source line primary
 linecode b8zs
 pri-group timeslots 1-24
 fdl ansi
!
controller T1 3
 framing esf
 linecode b8zs
 pri-group timeslots 1-24
 fdl ansi
!
!
voice-port 2:D
 !
voice-port 3:D
```

Note The voice-port 2:D and voice-port 3:D, correspond to controller T1 2 and controller T1 3, respectively, since they are configured as PRI, and therefore the “D” activates the D-channel.

```
interface Serial2:23
 description "PRI D channel"
 no ip address
 no ip directed-broadcast
 no keepalive
 isdn switch-type primary-ni
 isdn incoming-voice modem
 no fair-queue
 no cdp enable
!
interface Serial3:23
 description "PRI D channel"
 no ip address
 no ip directed-broadcast
 no keepalive
 isdn switch-type primary-ni
 isdn incoming-voice modem
 no fair-queue
 no cdp enable
```

Note Neither “interface Serial0:23” nor “interface Serial1:23” appear in this configuration, because the corresponding “controller T1 0” and “controller T1 1” are configured as T1s, and therefore do not correspond to a serial*x*:23 assignment.

T1 CAS FGB

```
controller T1 1
 ds0-group 1 timeslots 1-24 type e&m-fgb

voice-port 1:1
```

Note See Configuration Fundamentals: Configuring T1 Signaling on a Cisco AS5300, page 4-3, for a more detailed example.

T1 CAS FGD

```
controller T1 0
 ds0-group 1 timeslots 1-24 type e&m-fgd

voice-port 0:1
```

Note See Configuration Fundamentals: Configuring T1 Signaling on a Cisco AS5300, page 4-3, for a more detailed example (except for the different feature group).

CHAPTER 5

Provisioning SS7-Based POPs

Overview

POPs that must support the signaling provided by the PSTN require a different implementation. The progress and alerting tones that we are familiar with in traditional telephone services, such as dial or busy tones, are produced by the PSTN. In addition, telecommunications switches, such as the Class 4 and Class 5, communicate with each other through standards-based signaling. This signaling is essential to providing interconnections among carrier, cellular, and wireless networks, because it is the means by which calls are set up and torn down.

A major breakthrough in signaling networks was the separation of the signaling path from the voice or data path. This new data network, called common channel interoffice signaling, or CCS (also known as out-of-band signaling), overlays the carrier's switching network. CCS increases network intelligence, efficiency, automation, and functionality.

CCS has evolved into a standard called Signaling System 7, or SS7, a protocol that lowered costs and increased network reliability even further. With SS7, all carriers can interoperate as a consistent, seamless network. Services such as global billing, wireless roaming, and 800 number calling rely on the SS7 protocol to exchange messages reliably.

Where these services exist they must be maintained, although traffic now traverses the Internet instead of the traditional switched network. This is why Cisco developed the Cisco H.323 VoIP with SS7 Solution, to provide interconnection between SS7-based carriers and IP-based networks. H.323 is an ITU-T standard that is really a set of standards that define real-time multimedia communications for packet-based networks, otherwise known as IP telephony. Of particular interest are the call setup and control features provided by H.323.

Note Where SS7 must be supported, the Cisco Wholesale Voice Solution relies on the Cisco SS7 Interconnect for Voice Gateways Solution. That solution is a distributed system that provides SS7 connectivity for H.323 VoIP access gateways, by using the Cisco Signaling Controller (also known as the Cisco SC2200) and access gateways as a bridge from the H.323 IP network to the PSTN. The Cisco SS7 Interconnect for Voice Gateways Solution interacts over the IP network with other Cisco H.323 VoIP access gateways; it can also interoperate with H.323 endpoints by using non-SS7 signaling, as in ISDN PRI and channelized T1.

For the most current information about SS7 connectivity as it relates to the Cisco Wholesale Voice Solution, see the discussion of the Cisco SS7 Interconnect for Voice Gateways Solution, Release 1.1. That solution is described in detail at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/access/sc/rel7/soln/voip11/index.htm

A variety of topics are discussed at the above site, among them the following:

- An introduction to the Cisco SS7 Interconnect for Voice Gateways Solution, and its options
- How to install, provision, and configure required components
- How to use the features of the related software

Note The cross connections (channel assignments) in a Cisco SS7 Interconnect for Voice Gateways Solution are nailed up. That is, there is no dynamic assignment of cross connections on the basis of number prefix, hunt group, and so on.

This chapter does not attempt to recreate the substantial background information available at the Cisco SS7 Interconnect for Voice Gateways Solution website, although it does introduce the required components (see Cisco SC2200 Node Components, page 5-4). Although this chapter introduces the fundamentals of installing hardware and software, its main purpose is to focus on the provisioning details that are specific to Cisco SC2200 Signaling Link Controllers, Cisco Signaling Link Terminals (SLTs), and Cisco GWs in the Cisco Wholesale Voice Solution.

This chapter presents the following major topics:

- Architecture
- Configuring the Cisco SC2200 Node Components
- Installing Cisco SC2200 Node Hardware and Software

Architecture

The Cisco SC2200 logical entity consists of various components, and is referred to as a Cisco SC2200 *node*. This node, which appears as a Signaling Service Point (SSP) to the SS7 network, consists of an active and standby SC host, as well as a redundant pair of Cisco SLTs. The latter support SS7 A or F links, through redundant A and B link sets.

A links (access links) are used between the SSP and the STP, to provide access into the network and to databases (through the STP). With rare exceptions, there are always at least two A links, one to each of the STP pairs. F links (fully associated links) are used when a large amount of traffic must be handled between two SSPs, or when an SSP cannot be connected directly to an STP. F links allow SSPs to use the SS7 protocol to access SS7 databases even when it is not economical to provide a direct connection to an STP pair. Figure 5-1 illustrates the architecture of a Cisco SC2200 node.

Checkpointing monitors the states of the active and standby SC hosts, to enable switching from active to standby as needed. In the PSTN cloud, links are terminated by Service Switching Points (SSPs) or Signal Transfer Points (STPs). An SSP is the local exchange, and provides communication with a voice switch or SS7 switch. It also sends database queries throughout the SS7 network. An STP is essentially a router in the SS7 network, allowing SS7 message packets to travel from one SSP to another. An STP can be adjunct to a voice switch, although ideally it is a standalone function.

To provide SS7 connectivity for access gateways, the Cisco H.323 VoIP system architecture uses the SC2200 as a protocol translator, with SS7 signaling provided through the ISDN Q.931+ protocol (which in turn is tunneled through IP).

Table 5-1 lists the components, both required and optional, of the Cisco H.323 system architecture in support of SS7.

Figure 5-1 Architecture of a Cisco SC2200 Node

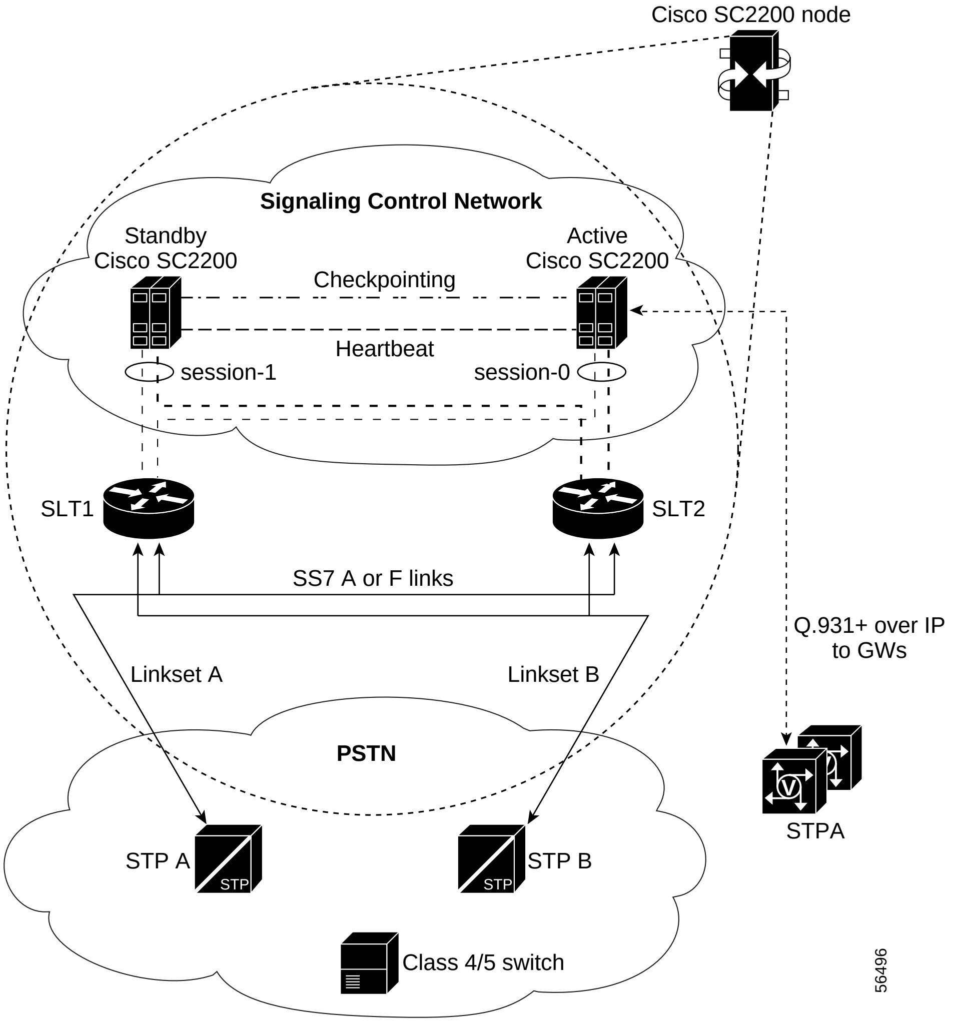


Table 5-1 Components of the Cisco H.323 VoIP System Architecture

Component	Description
Cisco Signaling Controller (SC)	*Required*. The Cisco SC2200, running MGC (SC) Software Release 7.4, operates as an SS7-to-ISDN protocol converter, a front end to the access gateways. The Cisco SC2200 is a Sun Netra series host that runs the Solaris operating system.
Cisco Signaling Link Terminal (SLT)	*Required*. The Cisco 2611 SLT terminates the physical SS7 links.
Cisco Access Gateway	*Required*. Cisco AS5300, Cisco AS5350, and Cisco AS5400 access gateways terminate voice and data ISUP (ISDN User Part) trunks.

Table 5-1 Components of the Cisco H.323 VoIP System Architecture (continued)

Component	Description
Cisco H.323 Gatekeeper	*Optional*. Cisco 3600s and 7200s are used to manage other nodes in an H.323 network.
Cisco LAN Switch	*Optional*. When necessary, switches from the Catalyst switch family are used to extend VLANs across platforms through backbone Fast Ethernet, Gigabit Ethernet, or ATM connections.

The Cisco SC2200 Signaling Controller is based on Sun Netra t 1120/1125 and t 1140/1145 series host computers (the “5” indicates AC-only operation); the Cisco SLT is based on the Cisco 2600 series routers. The combination of the Cisco SC and SLT in support of SS7 signaling over voice gateways form what is known as the Cisco SS7 Interconnect for Voice Gateways Solution.

Note The terms “SC” and “signaling controller” refer to the function of the Cisco SC2200 product as well as to the computers that perform the signaling conversion, the SC hosts. The term “MGC” (media gateway controller) is also used refer to the SC products and components when they are used in other solutions. MGC documents are later referred to with respect to the installation of SC node components.

Cisco SC2200 Node Components

The hardware components of the Cisco SC2200 node consist at the most fundamental level of a Cisco SC2200 Signaling Controller and Cisco Signaling Link Controller. Two sets of these are paired in a fault-tolerant SS7 signaling environment.

Note LAN switches, typically Catalyst 5000 and 6000 series switches, are optional, not mandatory, components of the Cisco Wholesale Voice Solution. For information about these switches, see Multilayer LAN Switches at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/lan/index.htm

The node components are described briefly below.

Cisco SC2200 Signaling Controller

The Cisco SC2200 host platform is essential to a Cisco Wholesale Voice Solution network that needs to support SS7 signaling. The Cisco SC2200 product is a signaling controller (SC) that converts telephony signals from one protocol variant to another. For example, it converts SS7 variants, such as ANSI SS7, to an IP-based variant required to establish calls between the PSTN and a packet data network. For detailed information about the Cisco SC2200, see the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/access/sc/rel7/index.htm

Cisco SLT

The Cisco SLT provides termination of the SS7 signaling. Based on the Cisco 2611 modular access router, the Cisco SLT terminates the lower layers of the SS7 protocol (MTP1 and MTP2), encapsulating the higher SS7 layers and reliably passing (backhauling) the IP packets (MTP layer 3) back to the Cisco SC2200 for interpretation and processing. By offloading the MTP1 and MTP2 layers from the Cisco SC2200, improvements are realized in both MTP2 performance and Cisco SC2200 system reliability and fault tolerance. For detailed information about the Cisco SLT, see the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/access/sc/slt/index.htm

Four MTP2 variants are supported or complied with:

- Telcordia (formerly Bellcore)/ANSI
- ITU-White, ITU-Blue
- Japan-NTT
- Japan Telecom TTC

Note The Cisco 2611 provides dual Ethernet interfaces. However, currently only a single Ethernet port is supported in the SLT configuration. Network modules are not supported, and only two SS7 links can be used.

Note Each Cisco SLT consists of a custom Cisco IOS image running on a Cisco 2611 router. However, the SLT itself does not function as a router. It is designed to offload signaling at layers MTP1 and MTP2 from the signaling controller. It is not designed to transport or tunnel SS7 over IP protocols other than RUDP (Reliable User Datagram Protocol).

The Cisco 2611 only has SS7 functionality when used as a Cisco SLT. All standard Cisco 2611 software features are disabled when the system is running the Cisco SLT image.

The Cisco SLT uses RUDP, a Cisco proprietary protocol that makes UDP reliable. RUDP connections are established by the RUDP client, which, in the case of the SLT, is the Session Manager. The SLT Session Manager maintains the connection between the SC and the SLT. Based on standard UDP functions, RUDP becomes reliable through the addition of the following TCP/IP features:

- The establishment and maintenance of reliable connections between client and server
- Flow control
- Congestion control
- The establishment of a reliable connection between an SLT and an SC by means of a TCP/IP address and a specified UDP port

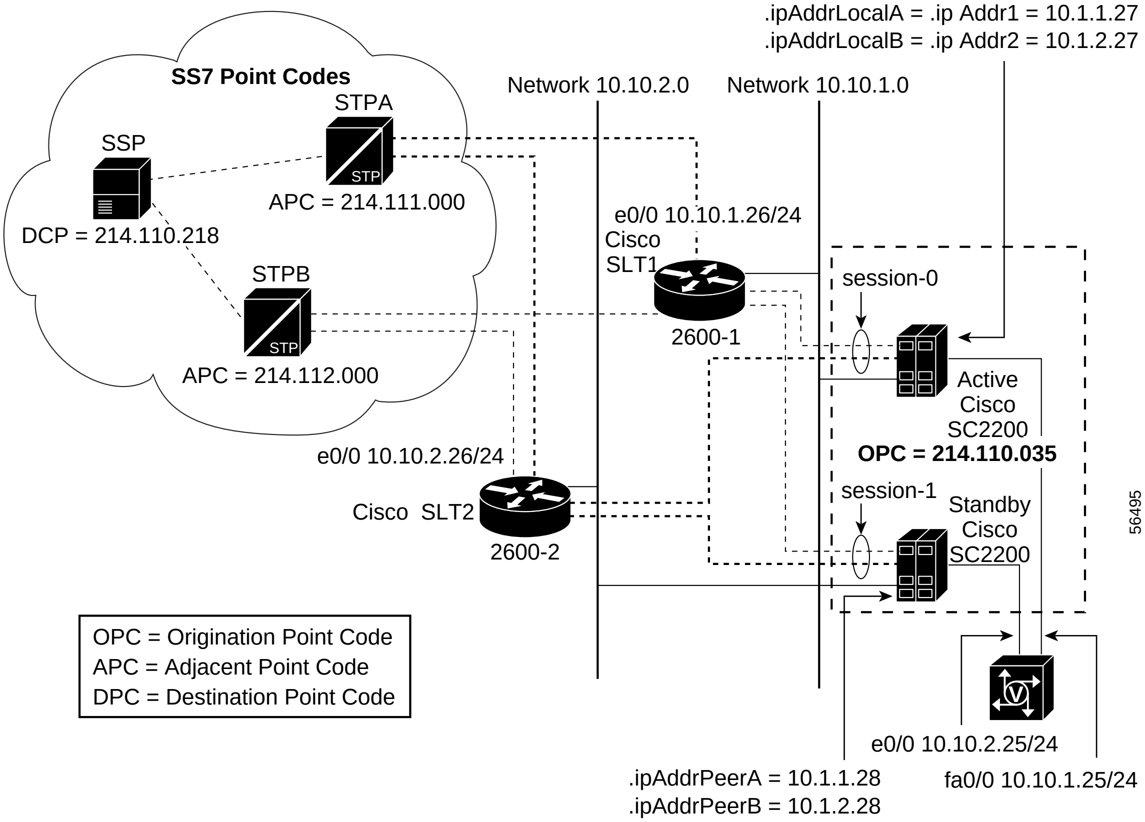
Configuring the Cisco SC2200 Node Components

The following discussion assumes that the necessary hardware have already been installed. For installation instructions, see Installing Cisco SC2200 Node Hardware and Software, page 5-30.

Figure 5-2 illustrates our example Cisco SC2200 node and its components for the following example configuration. (This figure is essentially the same as Figure 5-1, except for being rotated 90 degrees.) The addresses required for signaling in a redundant configuration are discussed in Edit the File XECfgParm.dat, page 5-7. Point codes are discussed in Create the File config.mml, page 5-10.

Caution For purposes of illustration, only a few examples of the network entities are illustrated in the discussion that follows. To facilitate provisioning, research your network needs carefully, and record all entities, their IP addresses, and SS7 point codes on a network map before continuing.

Figure 5-2 Example Cisco SC2200 Node and Components



Configuring the Cisco Signaling Controllers

You must configure both a designated active (primary) and designated standby (secondary) Cisco Signaling Controller (the Cisco SC2200), as in the procedures below:

- Configuring the Designated Active Cisco SC2200
- Configuring the Designated Standby Cisco SC2200

You must do the following on both machines:

- Assign User mgcuser to User Group mgcgroup
- Edit the File XECfgParm.dat
- Create the File config.mml

Refer to Figure 5-2 on page 5-6 for the following discussion.

Note If the necessary hardware and software have not yet been installed, proceed first to Installing Cisco SC2200 Hardware and Software, page 5-30.

Configuring the Designated Active Cisco SC2200

The example below illustrates the configuration on the designated active SC. With respect to network addresses, the configurations are essentially mirrors of each other, as each is the (failover) peer of the other.

Assign User *mgcuser* to User Group *mgcgroup*

To enable the software to be used by a regular user other than the superuser, you must log in on completion of the last reboot and assign the Signaling Controller users to belong to the group *mgcgroup*.

Step 1 Go to the directory */etc* and use a text editor such as vi to edit the file *group*, adding user *mgcuser* to user group *mgcgroup* as follows:

```
nobody::60001:
noaccess::60002:
nogroup::65534:
mgcuser::20000:mgcgroup
```

Note In the above example, we simply assign user *mgcuser* to group *mgcgroup*. The username *mgcuser* can be anything.

Step 2 Log out and log in as user *mgcgroup* to begin provisioning the Cisco SC2200.

Edit the File *XECfgParm.dat*

The file *XECfgParm.dat* on the Cisco SC2200 host contains a variety of configuration parameters that you must edit for your system to function. Refer to Figure 5-2 on page 5-6 for the following example.

Note For a complete list of parameters, including their functions, definitions, and sample values, see XECfgParm.dat File Parameters at the following URL:
http://www.cisco.com/univercd/cc/td/doc/product/access/sc/rel7/sw_ref/elparms.htm

The most current release of the SC software (also referred to as MGC, or Media Gateway Controller, software) is Release 7.4. Refer to discussions of the most recent version only.

Then find the file *XECfgParm.dat*, in */opt/CiscoMGC/etc* on the Cisco SC2200 host, then search for and edit the following parameters. Use a text editor such as vi.

Step 1 Edit the first local IP address, **.ipAddrLocalA*:

```
*.ipAddrLocalA = 10.10.1.27
```

This is the first IP address of the designated active, or primary, Cisco SC2200 host.

The local IP address is used for checkpointing and failover heartbeats with active/standby hosts.

Note This address is typically the same as that of **.IP_Addr1* (see below).

Step 2 Edit the second local IP address, **.ipAddrLocalB*:

```
*.ipAddrLocalB = 10.10.1.27
```

This is the second IP address of the designated active, or primary, Cisco SC2200 host. It is the same as that of **.ipAddrLocalA*.

Note If your configuration does not use an external card, leave this setting at the default value, 0.0.

Step 3 Edit the first corresponding peer's IP address, **.ipAddrPeerA*:

```
*.ipAddrPeerA = 10.10.1.28
```

The peer IP address is used for checkpointing (the mirroring of call state information on the other SC) and failover heartbeat (regular keep-alive status messages). With two Cisco hosts in a failover configuration, the peer IP address is one of two IP addresses of the second host.

Step 4 Edit the second corresponding peer's IP address, **.ipAddrPeerB*:

```
*.ipAddrPeerB = 10.10.2.28
```

Note If your configuration does not use an external card, leave this setting at the default value, 0.0.

Step 5 Edit the IP address of interface 1:

```
*.IP_Addr1 = 10.10.1.27
```

This is the same as the local address (**.ipAddrLocalA*) of the first interface (used for signaling).

Step 6 Edit the IP address of interface 2:

```
*.IP_Addr2 = 10.10.2.27
```

This is the same as the local address (**.ipAddrLocalB*) of the second interface (used for signaling).

Step 7 Edit the number of the port used between peer components or processes:

```
*.stPort = 7000
```

This can be the number of any unused port. This is the number of the port that communicates with the Cisco SLT.

Step 8 Edit a variety of additional parameters, as discussed below:

a. Determine the platform state (**.desiredPlatformState*). As we have an active and a standby SC host, we select **master** for the designated active unit:

```
*.desiredPlatformState master
```

Note We must edit this parameter to **slave** on the designated standby unit.

b. Enable checkpointing (**.SyscheckpointEnabled*). This ensures that calls that are in the talking state are preserved and survive a control switchover. All status checkpointing information is sent to the replicator on the active side.

```
*.SyscheckpointEnabled = true
```

c. Several connection types are supported, one of which is to the *failover daemon* (foverd). The daemon must be aware of A and B local and peer ports. Use the following values for the two required connections:

```
# connection 1 parameters
foverd.conn1Type = socket
foverd.ipLocalPortA = 1050
foverd.ipPeerPortA = 1051

# connection 2 parameters
foverd.conn2Type = socket
foverd.ipLocalPortB = 1052
foverd.ipPeerPortB = 1053
```

Note The above commented-out “connection 1” and “connection 2” lines are not required, but are useful in identifying the separate connection types.

Step 9 Examine the configuration. In our example configuration, we expect to see the following address assignments at a minimum in the file *XECfgParm.dat* on the primary host.

```
*.ipAddrLocalA = 10.1.1.27
*.ipAddrLocalB = 10.1.2.27
*.ipAddrPeerA = 10.1.1.28
*.ipAddrPeerB = 10.1.2.28


*.IP_Addr1 = 10.1.1.27
*.IP_Addr2 = 10.1.2.27
*.IP_Addr3 = 0.0.0.0
*.IP_Addr4 = 0.0.0.0

*.stPort = 7000
```

Note For the changes to the file *XECfgParm.dat* to take effect, you must restart the SC. For now, continue with the following step, and restart the SC when you are finished with all required provisioning. You do not need to restart the machine after other provisioning.

Prepare the Designated Standby Cisco SC2200 for Autoprovisioning

The most efficient way to provisioning the designated standby SC host is to enable a data synchronization parameter on both machines. This way, the only configuration required on the designated standby SC host is to edit the file *XECfgParm.dat*.

Step 1 The synchronization parameter in the file *XECfgParm.dat* is **pom.dataSync**, and you simply set it to **true** on the current machine:

```
pom.dataSync = true
```

As it comes up, the designated standby SC host will automatically pull the latest MML provisioning information from the active machine.

Step 2 You will need to edit the synchronization parameter on the designated secondary SC host when you edit the file *XECfgParm.dat* on that machine. (See Configuring the Designated Standby Cisco SC2200, page 5-18.) The *only* configuration that is required on the designated standby SC host is editing *XECfgParm.dat*. This will take care of the MML provisioning requirements for that machine.

For now, continue configuring the current machine. Proceed to Create the File config.mml, below.

Note When you are finished configuring the current (designated active) machine, restart the machine for the changes to *XECfgParm.dat* to take effect, then proceed to Configuring the Designated Standby Cisco SC2200, page 5-18.

Create the File *config.mml*

See Example Cisco SC2200 Node and Components, page 5-6. The following example steps address the principle components of an MML provisioning session on the designated active (primary) Cisco SC2200. You must also do this for the secondary SC in a fault-tolerant configuration. The result of the session is a file called *config.mml*. Only the key parameters are discussed. For a more detailed discussion of MML, see “Configuring with MML” at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/access/sc/rel7/prvplan/02mmlprv.htm

Caution The following is an example only. PSTN switch types and their provisioning requirements will vary. Although optional, descriptions are important for maintenance and troubleshooting.

Define Cards, Interfaces, and Point Codes

Step 1 First invoke MML from a dumb terminal connected to the Cisco SC2200:

```
sc2200>mml
```

The mml prompt appears.

Step 2 Start a new provisioning session as follows:

```
mml>prov-sta::srcver=”new”,dstver=”new_config”
```

Note You must enclose value strings in quotes.

Step 3 Using the **prov-add** command, define and describe Ethernet cards, and assign each a slot.

```
mml>prov-add:CARD:NAME="en-0",DESC="Ethernet Card 0",TYPE="EN",SLOT=0
mml>prov-add:CARD:NAME="en-1",DESC="Ethernet Card 1",TYPE="EN",SLOT=1
```

Note the following parameters and their descriptions:

- *prov-add:CARD:* Defines the Ethernet card
- *NAME*: Name of the card
- *DESC*: Description of the card
- *TYPE*: Type of the card, EN (options are ATM, EN, PTI, V35)
- *SLOT*: Slot number of the card (0 for built-in Ethernet card)

Step 4 Define Ethernet interfaces for the above cards. The *CARD* values must correspond with those in Step 3.

```
mml>prov-add:ENETIF:NAME="en-0-lif0",DESC="EN LIF 0",CARD="en-0"
mml>prov-add:ENETIF:NAME="en-1-lif1",DESC="EN LIF 1",CARD="en-1"
```

Note the following parameters and their descriptions:

- *prov-add:ENETIF*: Defines the properties of the Ethernet card
- *NAME*: Name of the interface
- *DESC*: Description of the interface
- *CARD*: Ethernet card name defined previously

Step 5 Define and describe a point code for the origination point code (OPC). This is the PSTN network address of *both* the primary and secondary Cisco SC2200s.

Note You must obtain point codes from Telcordia Technologies (formerly Bellcore) at http://www.telcordia.com, or from a third-party representative that interfaces with Telcordia, such as Illuminet at http://www.illuminet.com.

```
mml>prov-add:PTCODE:NAME="opc",DESC="Own Pointcode
214.110.035",NETADDR="214.110.35",NETIND=2
```

Note NETIND = 2 is a default value.

Step 6 Define and describe point codes for each destination point code (DPC) with which the SC communicates. DPCs include PSTN switches and SS7 route sets. Here we use the example of a Nortel DMS-100 switch.

```
mml>prov-add:PTCODE:NAME="dpc-dms100",DESC="dms100 point code
214-110-218",NETADDR="214.110.218",NETIND=2
```

Note the following parameters and their descriptions:

- *prov-add:PTCODE*: Defines the SS7 Point Code of the SC.
- *NAME*: Name of the point code
- *DESC*: Description of the point code
- *NETIND*: Network indicator, 2 in this case. (Options: 1 = CCITT or international, 2 = national)
- *NETADDR*: Network address of the SC.

Define SS7 Paths and Their Properties

Define an SS7 path and assign *sigsvsprop* (signaling service property) values for communication to each of the PSTN switches. Later we will define the switch entities from which the paths are derived.

Step 1 Define an SS7 path and signaling service properties for the Nortel DMS-100 switch, *ss7-dms100*.

```
mml>prov-add:SS7PATH:NAME="ss7-dms100",DESC="ss7 ansi standard to
dms100",DPC="dpc-dms100",
MDO="ANSISS7_STANDARD",CUSTGRPID="0000",CUSTGRPTBL="0101",SIDE="network"
mml>prov-add:sigsvcprop:name="ss7-dms100",BTermStartIndex="2"
mml>prov-add:sigsvcprop:name="ss7-dms100",BOrigStartIndex="1"
mml>prov-add:sigsvcprop:name="ss7-dms100",CLIPEss="1"
mml>prov-add:sigsvcprop:name="ss7-dms100",ReleaseMode="Sync"
```

Note the following parameters and their descriptions:

- *prov-add:SS7PATH*: Defines a SS7 signaling path to the DMS-100 switch
- *NAME*: Name of the signaling path
- *DESC*: Description of the signaling path
- *MDO*: MDO file name for the ANSI SS7 protocol
- *DPC*: SS7 point code name of the switch
- *CUSTGRPID*: A flag used for dial plan screening (A and B listing)
- *CUSTGRPTBL*: A file that hold CUSTGRPID data; numbers are mapped to dial plan files
- *prov-add:sigvcprop*: Defines signaling service properties, where
  - *BTermStartIndex*: 2 is a common default value
  - *BOrigStartIndex*: 1 is a common default value
  - *CLIPEss*: 1 is a common default value
  - *ReleaseMode*: Always use Sync.

Caution Take care to assign ReleaseMode="Sync" throughout. This improves call success rates.

Step 2 Define SS7 paths for all other switches as required. Parameters are as defined previously.

Defining External Nodes

The *EXTNODE* parameter is used to name the physical entities in the network, both switches and access gateways.

Step 1 The following assigns a name to the switch for which we assigned a point code in Define SS7 Paths and Their Properties, page 5-12.

```
mml>prov-add:PTCODE:NAME="dms100",DESC="Nortel DMS-100 switch",TYPE="DMS"
```

Note the following parameters and their descriptions:

- *prov-add:PTCODE*: Defines the switch or GW
- *NAME*: Name of the switch or GW
- *DESC*: Description of the switch or GW
- *TYPE*: Type of switch

Step 2 The following assigns a name to our Cisco AS5300 GW in a zone called Zone 1.

Note Organizing equipment into zones can be useful for management, but is not required. Choose names that are self-explanatory. Conventions can vary.

```
mml>prov-add:EXTNODE:NAME="z1-5300-1",DESC="zone 1 5300-1",TYPE="AS5300"
```

Define APCs, Linksets, SS7 Routes, and NAS Paths

The following steps define APCs (adjacent point codes), SS7 routes, and NAS paths, respectively.

Step 1 Define APCs to signal transfer points (STPs). STPs provide for signaling redundancy in the SS7 network. The following are for STPs A and B, respectively.

Note You must obtain point codes from Telcordia Technologies (formerly Bellcore) at http://www.telcordia.com, or from a third-party representative that interfaces with Telcordia, such as Illuminet at http://www.illuminet.com.

```
mml>prov-add:APC:NAME="apc-stpa",DESC="apc of stpa
214.111.000",NETADDR="214.111.0",NETIND=2
mml>prov-add:APC:NAME="apc-stpb",DESC="apc of stpb
214.112.000",NETADDR="214.112.0",NETIND=2
```

Note the following parameters and their descriptions:

- *prov-add:APC*: Defines the adjacent point code at which the GW terminates
- *NAME*: Name of the point code
- *DESC*: Description of the point code
- *NETADDR*: The adjacent point code
- *NETIND*: Network indicator, 2 in this case. (Options: 1 = CCITT or international, 2 = national)

Note *NETADDR* is similar but not identical to OPC, APC, or DPC, being an MML parameter.

Step 2 Define linksets. These are communication paths between the Cisco 2611 SLT and the STPs.

```
mml>prov-add:LNKSET:NAME="ls-stpa",DESC="linkset to stpa via
2600",APC="apc-stpa",PROTO="SS7-ANSI",TYPE="IP"
mml>prov-add:LNKSET:NAME="ls-stpb",DESC="linkset to stpb via
2600",APC="apc-stpb",PROTO="SS7-ANSI",TYPE="IP"
```

Note the following parameters and their descriptions:

- *prov-add:LNKSET*: Defines an SS7 linkset to the STP through the Cisco 2611 SLT
- *NAME*: Name of the linkset
- *DESC*: Description of the linkset
- *APC*: The point code at which the linkset terminates
- *PROTO*: The signaling protocol
- *TYPE*: Transport type of the linkset. It is TDM in this case (options: TDM, IP)

Step 3 Define SS7 routes. These are redundant signaling paths that relate the OPC to the DPC.

```
mml>prov-add:SS7ROUTE:NAME="rs-dms100-a",DESC="ss7 routeset to dms100 via the stpa dpc of
dms100 214-110-218",OPC="opc",DPC="dpc-dms100",LNKSET="ls-stpa",PRI=1
mml>prov-add:SS7ROUTE:NAME="rs-dms100-b",DESC="ss7 routeset to dms100 via the stpb dpc of
dms100 214-110-218",OPC="opc",DPC="dpc-dms100",LNKSET="ls-stpb",PRI=1
```

Note the following parameters and their descriptions:

- *prov-add:SS7ROUTE*: Defines an SS7 route to the switch
- *NAME*: Name of the route
- *DESC*: Description of the route
- *OPC*: Origination SS7 point code; the PC defined in *prov-add:PTCODE* for the SC. See Define Cards, Interfaces, and Point Codes, page 5-10.
- *DPC*: Destination SS7 point code; the PC defined in *prov-add:PTCODE* for the associated switch.
- *LNKSET*: The linkset that is associated with this route. It is the SS7 linkset defined in *prov-add:LNKSET* in this case.

Step 4 Define the ISDN signaling path to the NAS, the links from the SC to the network access servers, or GWs in our case. The key parameter is NASPATH, which includes an (arbitrary) description, an EXTNODE assignment (for the NAS), and a signaling protocol (MDO). There are a variety of protocols; here we use Bell 1268 C3 ISDN protocol.

```
mml>prov-add:NASPATH:NAME="ip-z1-5301",DESC="ISDN PRI over ip to 5300-1 in zone
1",EXTNODE="z1-5300-1",MDO="BELL_1268_C3"
mml>prov-add:sigsvcprop:name="ip-z1-5301",BcInitState="OOS"
```

Note the following parameters and their descriptions:

- *prov-add:NASPATH*: Defines an ISDN signaling path to the gateway
- *NAME*: Name of the signaling path
- *DESC*: Description of the signaling path
- *EXTNODE*: The gateway the signaling path is connected to
- *MDO*: MDO file name for the Bell 1268 ISDN protocol

Caution Recall that this is a nailed-up configuration. The Bell 1268 C3 protocol must be used in nailed-up configurations.

Define C7 IP Links and IP Links

The C7 IP link is used to define SS7 A-links between STPs A and B and the Cisco 2611 (SLT). The IP link is used to define the ISDN signaling paths (A and B, main and standby) between the GW (NAS) and the Cisco SLT. The STPs are redundant and provide load sharing for calls through two SLTs.

Note The Cisco Wholesale Voice Solution supports multiple RLM (Redundant Link Manager) groups for GWs only, not for the SLTs. For information about RLM, see Redundant Link Manager (RLM) at the following URL:
http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120t/120t3/rlm_123.htm

Step 1 Assign C7 IP links. The parameter *IPADDR* here must map to the same parameter in Step 2, below.

```
mml>prov-add:C7IPLNK:NAME="c7-2601-0a",DESC="ss7 a-link to stpa via 2600-1 slc
0",LNKSET="ls-stpa",IF="en-0-lif0",IPADDR="IP_Addr1",PORT=7000,PEERADDR="10.10.1.26",SLC=0
,PRI=1,TIMESLOT=0,NEXTHOP="0.0.0.0",NETMASK="255.255.255.255"
mml>prov-add:C7IPLNK:NAME="c7-2601-0b",DESC="ss7 a-link to stpb via 2600-1 slc
0",LNKSET="ls-stpb",IF="en-0-lif0",IPADDR="IP_Addr1",PORT=7000,PEERADDR="10.10.1.26",SLC=0
,PRI=1,TIMESLOT=1,NEXTHOP="0.0.0.0",NETMASK="255.255.255.255"
mml>prov-add:C7IPLNK:NAME="c7-2602-0a",DESC="ss7 a-link to stpa via 2600-2 slc
1",LNKSET="ls-stpa",IF="en-1-lif1",IPADDR="IP_Addr2",PORT=7000,PEERADDR="10.10.2.26",SLC=1
,PRI=1,TIMESLOT=0,NEXTHOP="0.0.0.0",NETMASK="255.255.255.255"
mml>prov-add:C7IPLNK:NAME="c7-2602-0b",DESC="ss7 a-link to stpb via 2600-2 slc
1",LNKSET="ls-stpb",IF="en-1-lif1",IPADDR="IP_Addr2",PORT=7000,PEERADDR="10.10.2.26",SLC=1
,PRI=1,TIMESLOT=1,NEXTHOP="0.0.0.0",NETMASK="255.255.255.255"
```

Note the following parameters and their descriptions:

- *prov-add:C7IPLNK*: Defines a C7 IP link to the SLT.
- *NAME*: Name of the link
- *DESC*: Description of the link
- *IF*: Ethernet interface defined in *prov-add:ENIF*
- *IPADDR*: IP address of the local machine
- *PORT*: UDP port for SS7 backhaul on the local machine (the SC)
- *PEERADDR*: IP address of the SLT
- *PEERPORT*: UDP port for SS7 backhaul on the SLT
- *PRI*: Priority
- *SLC*: Signaling link code
- *LNKSET*: SS7 linkset for this C7 IP link
- *TIMESLOT*: Serial interface number on the SLT. The designation is 0 for serial 0/0, 1 for serial 0/1, 2 for serial 1/0, and 3 for serial 1/1.

Caution The parameter **.stPort* in file *XECfgParm.dat* must also be configured to correspond to the local UDP port. On the primary (designated active) SC, make sure that **.stPort* = 7000. Port 7000 is the primary port. A standby port would be assigned 7001. See Edit the File XECfgParm.dat, page 5-7.

Step 2 Assign IP links.

```
mml>prov-add:IPLNK:NAME="z1-531-10",DESC="ip link for nas service to z1 5300-1
10",SVC="ip-z1-5301",IF="en-0-lif0",IPADDR="IP_Addr1",PORT=3001,PEERADDR="10.10.1.25",
PEERPORT=3001,PRI=1,SIGSLOT=0,SIGPORT=0,NEXTHOP="0.0.0.0",NETMASK="255.255.255.255"
mml>prov-add:IPLNK:NAME="z1-531-100",DESC="ip link for nas service to z1 5300-1
100",SVC="ip-z1-5301",IF="en-1-lif1",IPADDR="IP_Addr2",PORT=3001,PEERADDR="10.10.2.25",
PEERPORT=3001,PRI=1,SIGSLOT=0,SIGPORT=0,NEXTHOP="0.0.0.0",NETMASK="255.255.255.255"
```

Note the following parameters and their descriptions:

- *prov-add:IPLNK*: Defines an IP link for the ISDN signaling path defined in *prov-add:path*
- *NAME*: Name of the link
- *DESC*: Description of the link
- *IF*: Ethernet interface for the link defined in *prov-add:ENETIF*
- *IPADDR*: IP address of the Ethernet interface
- *PORT*: UDP port number for ISDN over IP
- *PEERADDR*: IP address of the Ethernet interface for ISDN over IP on the gateway
- *PEERPORT*: UDP port number for ISDN over IP on the gateway

Caution You must assign either 3001, 3003, 3005, or 3007 to *PEERPORT*. The *default* for a NAS (network access server, or GW) is 3001.

Importing a Trunk File

After defining all the signaling components in the previous steps, you must define the mapping between the CICs (Carrier Identification Codes) on the SS7 side and the bearer channels on the GW (ISDN over IP) side. There are two methods to accomplish this task: using the MML **prov-add:files** command or the **prov-add:nailtrnk** command. These are presented below.

Note By default, the trunk file is assumed to be stored on the Cisco SC2200 in */opt/CiscoMGC/etc/cust_specific*.

Option 1: Using the **prov-add:files** *Command*

Step 1 Use the command **prov-add:files** to import a trunk group file for use by the system. In the following example, a trunk mapping file named *export_trunk.dat* is referenced.

```
mml>prov-add:files:name="bcfile",file="cfg-mar17/export_trunk.dat",action="IMPORT"
```

The file to be imported looks like the following file for an example GW:

Note The keyword *#format2* must be present on the first line of a trunk group file.

```
#format2 - 0   <---this line is required
1  ss7-dms100 ffff  1  ip-z1-5301  0  1
2  ss7-dms100 ffff  2  ip-z1-5301  0  2
3  ss7-dms100 ffff  3  ip-z1-5301  0  3
4  ss7-dms100 ffff  4  ip-z1-5301  0  4

<---snip--->

21  ss7-dms100 ffff  21  ip-z1-5301  0  21
22  ss7-dms100 ffff  22  ip-z1-5301  0  22
23  ss7-dms100 ffff  23  ip-z1-5301  0  23
24  ss7-dms100 ffff  24  ip-z1-5301  0  24
```

The seven columns of the above file (in an order that is unique to a Cisco SC) are defined as follows:

- Column 1: Order number
- Column 2: SS7 signaling path as defined in *prov-add:ss7path*
- Column 3: Source span ID. Always enter ffff.
- Column 4: SS7 CIC number.

Caution Ensure that the CIC here matches the CIC on the SC side, and also that it falls within the CIC range supported by the serving IXC (interexchange carrier) switch. You must confirm this with your telecommunications service provider.

- Column 5: ISDN/IP signaling path as defined in *prov-add:naspath*
- Column 6: Destination span ID. Range is an integer from 1 through 65535 or ffff (the default). This value is converted from decimal to hexadecimal, except when the value is ffff.

Note The above number for Column 6 must correspond with the value of *nfas-int* (Non-Facility Associated Signaling interface number) on the associated GW, as set by the command **isdn service**. It must match the number of interfaces that are defined on the GW. Multiple spans that are assigned to a GW will have multiple destination span IDs. However, the destination span is always 0 because the GW (NAS) is using NFAS, and Controller 0 is where the D-channel is located. For a detailed discussion of the parameter *nfas-int* and other dial-related commands and parameters, refer to the *Cisco IOS Dial Technologies Command Reference, Release 12.2*, at the following URL:
http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fdial_r/

- Column 7: ISDN time slot number. These are DS0 bearer time slots. The series begins with 1 for each span.

Note See the note and reference immediately preceding. The above number must correspond with the value for *b_channel* (set by the command **isdn service**) on the associated GW.

Note the following parameters and their descriptions:

- *prov-add:files*: Imports a file

- *name*: Type of file to be imported. It is a trunk group with the keyword *BCFile* in this case.
- *file*: Name of file to be imported.
- *action*: "Import," which instructs MML to import the file

Option 2: Using the **prov-add:nailtrnk** *command*

Step 2 The second method is to use the regular MML **prov-add:nailtrnk** command, as in the following example:

```
mml>prov-add:nailtrnk:name="1",srcsvc="ss7-svc-sc1",srcspan="ffff",srctimeslot=101,dstsvc=
"nassvc-gw2, dstspan="0000",dsttimeslot=1
```

Note the following parameters and their descriptions:

- *prov-add:nailtrnk*: Provisions an individual nailed-up bearer channel
- *name*: Trunk identifier. It must be an integer > 0.
- *srcsvc*: SS7 signaling path as defined in *prov-add:ss7path*
- *srcspan*: Source span ID. Set it to ffff for SS7.
- *srctimeslot*: SS7 CIC. Ensure that it matches with the CIC on the SC.
- *dstsvc*: ISDN signaling path as defined in *prov-add:naspath*
- *dstspan*: Destination span ID. Set it to 0 for ISDN over IP.
- *dsttimeslot*: ISDN bearer channel number. It begins with 1.

Timesaver The former method, Option 1, is highly recommended, because it reduces typing and introduces fewer errors.

Step 3 Whatever option you choose, copy the provisioning data to the production area (*/opt/CiscoMGC/etc*):

```
mml>prov-cpy
```

This command copies all the provisioning data and closes the provisioning session.

A copy of this configuration, except for the file *XECfgParm.dat*, is backed up and stored in */opt/CiscoMGC/etc/CONFIG_LIB/CFG_*<dstver>

where <dstver> is the destination version, and *CFG_ is* prepended automatically.

Configuring the Designated Standby Cisco SC2200

Now provision the designated standby (secondary) host. The only provisioning required on this machine is to edit the file *XECfgParm.dat*. The MML provisioning is taken care of by the synchronization parameter. (See Prepare the Designated Standby Cisco SC2200 for Autoprovisioning, page 5-10.)

Step 1 Refer to Configuring the Designated Active Cisco SC2200, page 5-7.

Step 2 Assign user *mgcuser* to user group *mgcgroup*, as in Assign User mgcuser to User Group mgcgroup, page 5-7.

Step 3 See Edit the File XECfgParm.dat, page 5-7. Edit the file *XECfgParm.dat* on the secondary host with the same parameters, with the following exceptions:

a. Change the value of the parameter **.stPort*.

> **Note** With two Cisco hosts in a failover configuration, you must enter a different value (for example, 7001) for **.stPort* in the file *XECfgParm.dat* on the secondary host.

b. Because this is the designated standby unit, we make it the *slave* unit, with the parameter **.desiredPlatformState*:

```
*.desiredPlatformState = slave
```

Step 4 Examine the configuration. In our example configuration, we expect to see the following address assignments at a minimum in the file *XECfgParm.dat* on the designated standby host.

```
*.ipAddrLocalA = 10.1.1.28
*.ipAddrLocalB = 10.1.2.28
*.ipAddrPeerA = 10.1.1.27
*.ipAddrPeerB = 10.1.2.27


*.IP_Addr1 = 10.1.1.28
*.IP_Addr2 = 10.1.2.28
*.IP_Addr3 = 0.0.0.0
*.IP_Addr4 = 0.0.0.0

*.stPort = 7001 <--- port number must be different from that on primary host
```

Step 5 Enable the synchronization parameter. This is as you set it in Prepare the Designated Standby Cisco SC2200 for Autoprovisioning, page 5-10.

```
pom.dataSync = true
```

As it comes up, the designated standby SC host will automatically pull the latest MML provisioning information from the active machine.

Step 6 Restart the machine to enable the changes to the file *XECfgParm.dat*.

Configuring the Cisco Signaling Link Terminals

This section presents the following major topics:

- Overview
- Configuring Basic Parameters on Both Cisco SLTs
- Configuring SLT1
- Configuring SLT2

> **Note** If the necessary hardware and software have not yet been installed, proceed first to Installing Cisco SLT Hardware and Software, page 5-34.

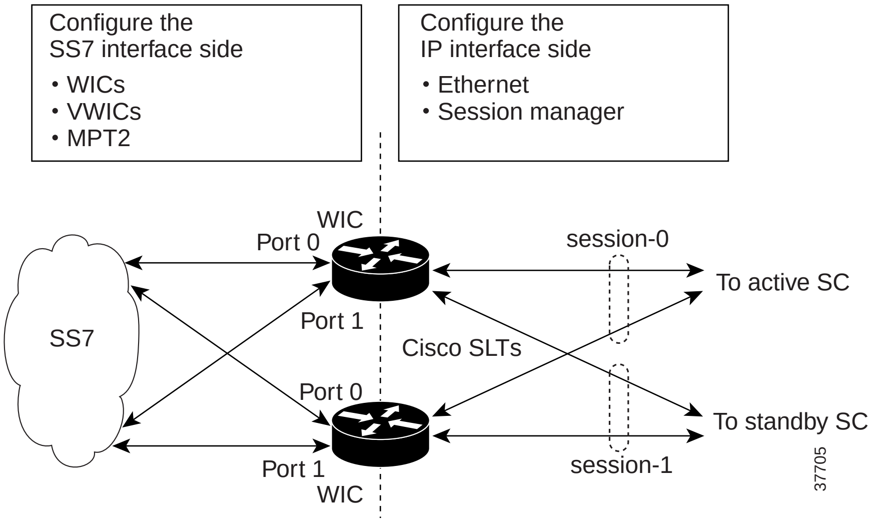
Overview

Because the Cisco SLTs communicate with both to the SS7 network as well as the SC host, there are two fundamental aspects of provisioning the SLTs:

- Configuring the SS7 interface side
- Configuring the IP interface side

Figure 5-3 illustrates these two aspects. The SS7 cloud contains STPs and SSPs, among other entities.

Figure 5-3 Two Aspects of Configuring the Cisco SLTs



With both SLTs set up to provide load sharing, they can both send calls to an active SC for call processing. In a fault-tolerant configuration, with both SLTs active simultaneously, we will refer to them simply as SLT1 and SLT2. A Session Manager facilitates the SS7 backhaul between the SLT and the SC. On each SLT, two sessions (maximum) can be configured:

1. The first session, **session-0**, is for SS7 backhaul to the standalone in a non-fault-tolerant case (*not recommended*) and to the active SC in our fault-tolerant case.
2. The second session, **session-1**, is for SS7 backhaul to the standby SC in our fault-tolerant case.

See our example in Figure 5-2 on page 5-6. We begin with the configuration of SLT1, then highlight the simple difference in the configuration of SLT2.

Caution Note the following exceptions and caveats:

- With the Cisco SLT, the SS7 MTP2 protocol is the *only* serial protocol supported. Therefore, you cannot configure serial interfaces for other protocols, such as HDLC, PPP, X.25, LAPB, and Frame Relay.
- The **encapsulation** interface configuration command is not supported on the Cisco SLT image. Also, all other commands related to non-SS7 serial protocols are not supported.
- Cisco recommends that you take MTP2 links out of service (OOS) at the Cisco SC2200 host before issuing Cisco SLT commands.

Configuring Basic Parameters on Both Cisco SLTs

This section applies to both SLTs. We use the example of SLT1 in Figure 5-2 on page 5-6.

Configuring a Cisco SLT is not quite the same as configuring a router. To configure the basic parameters of the Cisco SLT, complete the following steps:

Step 1 Power on the Cisco SLT.

Caution Do not press any keys until the system messages stop. Any keys pressed during this time are interpreted as the first command, which may cause the Cisco SLT to power off and start over. It will take a few minutes for these messages to stop.

Step 2 When you are asked if you would like to configure the initial configuration dialog, enter **y** (yes) to begin the configuration.

```
Would you like to enter the initial configuration dialog? [yes/no]: y
```

At any point you may enter a question mark for help. Use **Ctrl-c** to abort configuration dialog at any prompt. Default settings are in square brackets.

Basic management setup provides only enough connectivity for management of the system. Extended setup will ask you to configure each interface on the system.

Step 3 Enter **y** (yes) to enter basic management setup.

```
Would you like to enter basic management setup? [yes/no]: y
Configuring global parameters:
```

Step 4 Enter the host name for the Cisco 2611 router.

```
Enter host name [Router]: 2600-1
```

Step 5 Enter the enable secret password. This password is encrypted (more secure) and cannot be seen when viewing the configuration. The enable secret is a password used to protect access to privileged EXEC and configuration modes. This password, after entered, becomes encrypted in the configuration.

```
Enter enable secret: enable_secret
```

Step 6 Enter an enable password that is different from the enable secret password. This password is not encrypted (less secure) and can be seen when viewing the configuration. The enable password is used when you do not specify an enable secret password, with some older software versions, and with some boot images.

```
Enter enable password: enable_password
```

Step 7 Enter the virtual terminal password, which prevents unauthenticated access to the Cisco SLT through ports other than the console port. The virtual terminal password is used to protect access to the router over a network interface.

```
Enter virtual terminal password: vt_password
```

Step 8 Configure the SNMP parameters.

```
Configure SNMP Network Management? [yes]: no
Community string [public]:
```

Note We are not enabling SNMP in this example. SNMP is required to enable network management applications that use SNMP traps. See Enabling SNMP, page 3-11.

Step 9 Enter the interface name used to connect to the management network:

```
Current interface summary

Controller Timeslots D-Channel Configurable modes Status
T1 0/2     24        23        pri/channelized    Administratively up
T1 0/3     24        23        pri/channelized    Administratively up

Any interface listed with OK? value "NO" does not have a valid configuration

Interface                  IP-Address      OK? Method Status Protocol
Ethernet0/0                unassigned      NO  unset   up                   up
Serial0/0                  unassigned      NO  unset  down                  down
Ethernet0/1                unassigned      NO  unset   up                   down
Serial0/1                  unassigned      NO  unset  down                  down

Enter interface name used to connect to the management network from the above interface
summary: Ethernet0/0
```

Step 10 Configure the Ethernet interface:

```
Configuring interface Ethernet0/0:
Configure IP on this interface? [yes]: y
```

Step 11 Specify the IP address and the subnet mask for the interface:

```
IP address for this interface: 10.1.1.26
Subnet mask for this interface [255.0.0.0]: 255.255.255.0
Class A network is 10.0.0.0, 24 subnet bits; mask is /24
```

Step 12 Save configuration to NVRAM and exit the initial configuration mode.

```
The following configuration command script was created:

hostname 2600-1
enable secret 5 $1$0gLU$vLK1YHrMcianH5oVWFJNP/
enable password lablab
line vty 0 4
password lab
no snmp-server
!
no ip routing
!
interface Ethernet0/0
no shutdown
ip address 10.10.1.26 255.255.255.0
!
interface Serial0/0
shutdown
no ip address
!
interface Ethernet0/1
shutdown
no ip address
!
interface Serial0/1
shutdown
no ip address
!
```

```
end

[0] Go to the IOS command prompt without saving this config.
[1] Return back to the setup without saving this config.
[2] Save this configuration to nvram and exit.
Enter your selection [2]: 2
Building configuration...
Use the enabled mode 'configure' command to modify this configuration.

Press RETURN to get started!
```

This completes the basic configuration of SLT1.

Step 13 Repeat the above steps on SLT2, taking care to choose a different host name for the machine.

Configuring the Session Manager and RUDP

The Session Manager and the Reliable User Datagram Protocol (RUDP) are responsible for managing the communication sessions between the Cisco SLTs and the Cisco Signaling Controllers. Regardless of the number of SS7 links that the SC activates on the Cisco 2611, the SLT maintains only one Session Manager session with each of the Cisco SC2200s.

Caution You must reboot the SLT after setting a new session configuration or after changing existing session configuration. Do not change session timers unless instructed to do so by Cisco technical support. Changing timers may result in service interruption or outage.

Configuring the MTP2 Variant

As noted in Cisco SLT, page 5-5, SS7 MTP2 supports four variants. The parameters under one variant have different meanings, purposes, and ranges in another.

Note Note the following considerations:

- Parameters that are not configured will remain at the default values.
- The channel to be configured must be out of service at the Cisco SC2200 before the variant or the variant configuration can be changed.
- After the variant configuration changes have been made, the router must be reloaded to apply the changes.

Do the following in global configuration mode to establish the appropriate SS7 MTP2 variant.

Step 1 Set the amount of DRAM to be used for I/O memory to 40 percent.

Note If you do not set the I/O memory to at least 40 percent, there will not be enough memory for the SS7 MTP2 signaling.

```
2600-1(config)# mem iomem 40
```

Step 2 Configure the MTP2 Telcordia variant (formerly Bellcore) for channel 2.

```
2600-1(config)# ss7 mtp2-variant Bellcore 2
```

Note The term "Bellcore" is still used to represent the Telcordia Technologies variant.

The router prompt will change to **config-Bellcore**.

Step 3 Set the aligned timer to 30,000 milliseconds.

```
2600-1(config-Bellcore)# T3 30000
```

Step 4 Set the maximum number of MSUs waiting for acknowledgment to 16.

```
2600-1(config-Bellcore)# unacked-MSUs 16
```

Step 5 Set the excessive delay timer to 50,000 milliseconds.

```
2600-1(config-Bellcore)# T7 50000
```

Step 6 Exit Bellcore variant configuration mode.

```
2600-1(config-Bellcore)# exit
```

Step 7 Exit configuration mode.

```
2600-1(config)# end
```

Step 8 Save the running configuration to the startup configuration.

```
2600-1# copy running-config startup-config
```

Configuring SLT1

Configure I/O Memory Size

To provide sufficient memory to process SS7 messages, you must set the I/O memory size to at least 40%:

```
slt1(config)# memory-size iomem 40
```

Configure the Session Manager Session

For each session, the first IP address and UDP port are for the SC host, and the second address and port are for the SLT itself.

Step 1 Establish session-0, which communicates with the designated active Cisco SC2200. The first address and port are those of the designated active SC, followed by those of this SLT.

```
slt1(config)# ss7 session-0 address 10.10.1.27 7000
10.10.1.26 7000
REBOOT the router after saving new configuration
```

Note Note the reboot message above.

Step 2 Establish session-1 on the active SLT. The first address and port are those of the designated standby SC, followed by the address and *failover port* of this SLT.

```
slt1(config)# ss7 session-1 address 10.10.1.28 7000
```

```
10.10.1.26 7001
REBOOT the router after saving new configuration
```

Caution Make sure that these configurations match with those on both the Cisco SC2200s, or the sessions will never come up:

- In the fault-tolerant case, the remote UDP ports in both sessions must be the same value.
- Also in the fault-tolerant case, the local IP address in both sessions must be the same, because the SLT must support one Ethernet port for SS7 backhaul only. However, the local UDP port must be different.

Step 3 Reboot the SLT for the configuration to take effect.

Verify the Configuration

Do the following to ensure that the configuration is properly established.

Step 1 Verify the serial controllers, making sure both controllers are set to DTE.

```
slt1# show controller serial 0/0
Interface Serial0/0
Hardware is PowerQUICC MPC860
DTE V.35 TX and RX clocks detected.
idb at 0x80CA395C, driver data structure at 0x80CA98F0

<--- snip --->

slt1# show controller serial 0/1
Interface Serial0/1
Hardware is PowerQUICC MPC860
DTE V.35 TX and RX clocks detected.
idb at 0x80CB16D8, driver data structure at 0x80CB766C

<--- snip --->
```

Step 2 Verifying the serial interfaces, making sure the lines and protocols are up.

```
slt1# show interface serial 0/0
Serial0/0 is up, line protocol is up
Hardware is PowerQUICC Serial
MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec,
reliability 255/255, txload 5/255, rxload 1/255
Encapsulation SS7 MTP2, loopback not set
Keepalive set (10 sec)
Last input never, output 00:00:00, output hang never

<--- snip --->

slt1# show interface serial 0/1
Serial0/1 is up, line protocol is up
Hardware is PowerQUICC Serial
MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec,
reliability 255/255, txload 5/255, rxload 1/255
Encapsulation SS7 MTP2, loopback not set
Keepalive set (10 sec)
Last input never, output 00:00:00, output hang never
```

```
<--- snip --->
```

Step 3 Verify the Session Manager configuration. This command verifies the Session Manager sessions, including the IP addresses and UDP ports. Ensure that the addresses of the remote hosts (Cisco SC2200s) correspond with your network design.

```
slt1# show ss7 sm session
Session[0]: Remote Host 10.10.1.27:7000, Local Host
10.10.1.26:7000
retrans_t = 600
cumack_t = 300
kp_t = 2000
m_retrans = 2
m_cumack = 3
m_outseq = 3
m_rcvnum = 32

Session[1]: Remote Host 10.10.1.28:7000, Local Host
10.10.1.26:7001 <---the standby port on this host
retrans_t = 600
cumack_t = 300
kp_t = 2000
m_retrans = 2
m_cumack = 3
m_outseq = 3
m_rcvnum = 32
```

Step 4 When you have completed the configuration, remember to reboot the SLT for the configuration to take effect.

Step 5 Display the Session Manager statistics.

The show ss7 sm stats command provides you statistics of each Session Manager session, including the state. The following is a typical successful report. Errors will be flagged as nonzero.

```
slt1# show ss7 sm stats

-------------------- Session Manager --------------------

Session Manager state = SESSION SET STATE-ACTIVE
Session Manager Up count = 7
Session Manager Down count = 6
lost control packet count = 0
lost PDU count = 0
failover timer expire count = 5
invalid_connection_id_count = 0

Session[0] statistics SM SESSION STATE-ACTIVE:
Session Down count = 0
Open Retry count = 0

Total Pkts receive count = 9
Active Pkts receive count = 1
Standby Pkts receive count = 0
PDU Pkts receive count = 8
Unknown Pkts receive count = 0

Pkts send count = 9
Pkts requeue count = 0
-Pkts window full count = 0
-Pkts resource unavail count = 0
-Pkts enqueue fail count = 0
PDUs dropped (Large) = 0
PDUs dropped (Empty) = 0

RUDP Not Ready Errs = 0
RUDP Connection Not Open = 0
RUDP Invalid Conn Handle = 0
RUDP Unknown Errors = 0
RUDP Unknown Signal = 0
NonActive Receive count = 0

Session[1] statistics SM SESSION STATE-STANDBY: <---in a fault-tolerant application only
Session Down count = 0
Open Retry count = 86352

Total Pkts receive count = 0
Active Pkts receive count = 0
Standby Pkts receive count = 0
PDU Pkts receive count = 0
Unknown Pkts receive count = 0

Pkts send count = 0
Pkts requeue count = 0
-Pkts window full count = 0
-Pkts resource unavail count = 0
-Pkts enqueue fail count = 0
PDUs dropped (Large) = 0
PDUs dropped (Empty) = 0

RUDP Not Ready Errs = 0
RUDP Connection Not Open = 0
RUDP Invalid Conn Handle = 0
RUDP Unknown Errors = 0
RUDP Unknown Signal = 0
NonActive Receive count = 0
```

Step 6 To see the overall configuration, see An Overall Configuration: SLT1, below.

Step 7 Proceed to Configuring SLT2, page 5-28.

An Overall Configuration: SLT1

```
slt1# show start
Using 951 out of 29688 bytes
!
version 12.0
service timestamps debug datetime msec localtime
service timestamps log datetime msec localtime
no service password-encryption
!
hostname slt1
!
enable password cisco123
!
!
!
!
!
memory-size iomem 40
ip subnet-zero
!
!
!
!
```

```
interface Ethernet0/0
ip address 10.10.1.26 255.255.255.0
no ip directed-broadcast
full-duplex
!
interface Serial0/0
no ip address
no ip directed-broadcast
no ip mroute-cache
!
interface Ethernet0/1
no ip address
no ip directed-broadcast
shutdown
!
interface Serial0/1
no ip address
no ip directed-broadcast
!
ip classless
no ip http server
!
tftp-server flash
ss7 session-0 address 10.10.1.27 7000 10.10.1.26 7000
ss7 session-1 address 10.10.1.28 7000 10.10.1.26 7001 <---required for fault tolerance
ss7 mtp2-variant Bellcore 0
ss7 mtp2-variant Bellcore 1
ss7 mtp2-variant Bellcore 2
ss7 mtp2-variant Bellcore 3
!
line con 0
exec-timeout 0 0
transport input none
line aux 0
line vty 0 4
exec-timeout 0 0
no login
!
end
```

Configuring SLT2

See Figure 5-2 on page 5-6. The configuration of SLT2 is essentially identical to the configuration presented in Configuring SLT1, page 5-24, except for the address of the current SLT.

Configure the Session Manager Session

Step 1 Establish session-0 on SLT2.

```
slt2(config)# ss7 session-0 address 10.10.2.27 7000
10.10.2.26 7000
REBOOT the router after saving new configuration
```

Step 2 Establish session-1 on SLT2.

```
slt2(config)# ss7 session-1 address 10.10.2.28 7000
10.10.2.26 7001
REBOOT the router after saving new configuration
```

Step 3 When you have completed the configuration, remember to reboot the SLT for the configuration to take effect.

Step 4 To see the overall configuration, see An Overall Configuration: SLT2, below.

An Overall Configuration: SLT2

```
slt2# show start
Using 951 out of 29688 bytes
!
version 12.0
service timestamps debug datetime msec localtime
service timestamps log datetime msec localtime
no service password-encryption
!
hostname slt1
!
enable password cisco123
!
!
!
!
!
memory-size iomem 40
ip subnet-zero
!
!
!
!
interface Ethernet0/0
ip address 10.10.2.26 255.255.255.0
no ip directed-broadcast
full-duplex
!
interface Serial0/0
no ip address
no ip directed-broadcast
no ip mroute-cache
!
interface Ethernet0/1
no ip address
no ip directed-broadcast
shutdown
!
interface Serial0/1
no ip address
no ip directed-broadcast
!
ip classless
no ip http server
!
tftp-server flash
ss7 session-0 address 10.10.1.27 7000 10.10.1.23 7000
ss7 session-1 address 10.10.1.28 7000 10.10.1.23 7001 <---required for fault tolerance
ss7 mtp2-variant Bellcore 0
ss7 mtp2-variant Bellcore 1
ss7 mtp2-variant Bellcore 2
ss7 mtp2-variant Bellcore 3
!
line con 0
```

```
exec-timeout 0 0
transport input none
line aux 0
line vty 0 4
exec-timeout 0 0
no login
!
end
```

Installing Cisco SC2200 Node Hardware and Software

The following discussion addresses the Cisco SC2200 host server and the Cisco SLT.

Note The online documents referred to use the term “Media Gateway Controller” (MGC) in place of “SC” or “Cisco SC2200 node.” In any case, the role and function of the two entities is essentially the same. The following discussion concerns only the use of similar hardware and software.

Installing Cisco SC2200 Hardware and Software

Introduction

Table 5-3 lists the minimum hardware and software requirements for the Cisco SC2200 (simplex system).

Note Double hardware quantities for redundant systems, as required in SS7 environments.

The following is an abbreviated discussion that focuses on system-specific provisioning parameters with relation to a specific network-configuration example. For detailed information, refer to *Cisco MGC Release 7 Provisioning Guide*, at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/access/sc/rel7/swinst/index.htm

Note in particular the following chapters in the above document:

- “Installing the Operating System Software” (Chapter 1)
  (Installing the Sun Solaris 2.6 Operating System)
- “Installing the Cisco Media Gateway Controller Software Release 7.4” (Chapter 4)

Table 5-2 Minimum Hardware and Software Requirements for the Cisco SC2200

Hardware	Software
One Sun Ultra 5 SPARC workstation, with a minimum of 2048MB[1] of RAM and a 4 GB hard disk	Sun Solaris 2.6 Cisco Media Gateway Controller software Release 7.4

[1] The *install.sh* script will fail without this minimum of RAM.

Installing Cisco SC2200 Hardware

Step 1 Refer to the following Web site:

Cisco SS7 Interconnect for Voice Gateways Solution, Release 1.1, at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/access/sc/rel7/soln/voip11/index.htm

Note The following steps refer to documents at the above URL.

Step 2 Refer to the following online document at the *Cisco SS7 Interconnect for Voice Gateways Solution, Release 1.1* site:

Cisco Media Gateway Controller Hardware Installation Guide

Step 3 Refer to the following chapter in the above document:

"Cisco Media Gateway Controller Product Introduction"

a. In the section "Cisco SC2200 Product Overview," note the host platforms that support the Cisco SC2200, and select the appropriate host for your application.

b. In the section "Cisco MGC Product Configurations," note the host configuration options and select the appropriate option for your application.

Step 4 Refer to the following chapter in the *Cisco Media Gateway Controller Hardware Installation Guide*:

"Preparing the Installation Site"

Note the instructions that are specific to the hardware you have selected.

Step 5 Refer to the following chapter in the *Cisco Media Gateway Controller Hardware Installation Guide*:

"Hardware Installation Instructions"

a. Read the section "Installation Preview," and note the instructions that are specific to the hardware you have selected.

b. Read the section "Installing Host Hardware," and note the instructions that are specific to the hardware you have selected.

Step 6 Refer to the following chapter in the *Cisco Media Gateway Controller Hardware Installation Guide*:

"Cabling and Connections"

Connect your hardware components to the network as appropriate for your installation.

Step 7 Refer to the following chapter in the *Cisco Media Gateway Controller Hardware Installation Guide*:

"Power and Grounding"

Read the section "Connecting" for the host platform you have selected, and ensure that you observe the appropriate power and grounding requirements.

Installing Cisco SC2200 Software

Step 1 Refer to the following Web site:

Cisco SS7 Interconnect for Voice Gateways Solution, Release 1.1, at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/access/sc/rel7/soln/voip11/index.htm

Note The following steps refer to documents at the above URL.

Step 2 Refer to the following online document at the *Cisco SS7 Interconnect for Voice Gateways Solution, Release 1.1* website:

Cisco MGC Software Release 7 Installation & Configuration Guide

Step 3 Refer to the following chapter in the above document:

"Installing the Sun Solaris 2.6 Operating System"

Follow the instructions in the above chapter to install the required software.

Caution For the most current information, including the latest patches, always refer to the release notes for the software provided for your host platform.

Basic Provisioning of the Cisco SC2200

Note The following procedures require reasonable proficiency in UNIX, and must be done in superuser mode. The following commands are entered at the command prompt (represented by a generic ">").

Installing the Solaris Operating System

If the Solaris OS has not yet been installed, refer to "Installing the Sun Solaris 2.6 Operating System," Chapter 1 in *Cisco Media Gateway Controller Software Release 7 Installation and Configuration Guide*, at the following URL:

http:// www.cisco.com/univercd/cc/td/doc/product/access/sc/rel7/swinst/1inst_os.htm

The above website also covers the following topics:

- Booting from a local CD-ROM
- Loading the Sun Solaris 2.6 operating system (including disk partitioning
- Installing Sun Solaris patches
- Installing alarm management software
- Configuring a second Ethernet interface
- Configuring a second disk drive (including Volume Manager, to support mirroring of the operating system)
- Installing log and spool file systems

Uninstalling Preexisting Media Gateway Controller Software

You may need to uninstall existing software. If so, proceed as follows.

Step 1 Make sure the Cisco SC2200 software is not running. To stop the software, enter the following:

```
sc2200% /etc/init.d/CiscoMGC stop
```

Step 2 Go to the home directory where the Cisco SC2200 installation packages reside, then enter the following:

```
sc2200% uninstall.sh
```

Step 3 To ensure that all the old software packages are completely uninstalled, enter the following:

```
sc2200% pkginfo | grep CSC
```

Look for package files (with the*.pkg* extension). If packages are listed in the output, uninstall them manually by entering the following:

```
pkgrm package_name_without_.pkg_extension
```

Installing Signaling Controller Packages

Step 1 Go to the home directory where the Cisco SC2200 installation packages reside (*/opt/CiscoMGC*), then enter the following:

```
sc2200% sh install.sh
```

Step 2 As the install script proceeds, choose the following options in response to various questions that will appear:

a. Select the *BASE* directory for the installation (the default is */opt/CiscoMGC*.)

b. Use the *admin* file for automated installation, which overrides all install-time questions.

c. Select **UID** and **GID** for user *mgcuser* and group *mgcgroup*, which are created when the Utilities are installed.

Installing Patches (If Available)

The following procedure is necessary when patches are available. For the latest patches from Sun, refer to the following URL:

http://sunsolve.sun.com

Refer also to Installing the Sun Solaris Patches in “Installing the Sun Solaris 2.6 Operating System,” Chapter 1 in *Cisco Media Gateway Controller Software Release 7 Installation and Configuration Guide*, at the following URL:

http:// www.cisco.com/univercd/cc/td/doc/product/access/sc/rel7/swinst/1inst_os.htm

Assigning User *mgcuser* to User Group *mgcgroup*

To enable the software to be used by a regular user other than the superuser, you must log in upon completion of the last reboot and assign the Cisco SC2200 users to belong to the *mgcuser* group. See Assign User mgcuser to User Group mgcgroup, page 5-7.

Editing the File *XECfgParm.dat*

The file XECfgParm.dat contains a variety of parameters that must be edited for your system to function. See Edit the File XECfgParm.dat, page 5-7.

For a complete list of parameters, including their functions, definitions, and sample values, see the *Cisco Media Gateway Controller Software Release 7 Reference Guide* at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/access/sc/rel7/sw_ref/index.htm

Restarting and Provisioning the Cisco SC2200

Enter the following commands at the prompt.

Note The name of the host machine prompt will vary.

Step 1 First stop all processes (through procM, the process manager).

```
sc2200% /etc/init.d/CiscoMGC stop
```

The following appears:

```
Waiting for procM to exit

...shutdown complete
```

Step 2 Restart the software:

```
sc2200% /etc/init.d/CiscoMGC start
```

The following appears:

```
sc2200%

Provisioning the SC2200

Starting MML
```

This completes the basics of provisioning the Cisco SC2200 Signaling Controller. For the details of configuration, see Configuring the Cisco Signaling Controllers, page 5-7.

Installing Cisco SLT Hardware and Software

Installing Cisco SLT Hardware

Step 1 Refer to *Cisco SS7 Interconnect for Voice Gateways Solution, Release 1.1*, at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/access/sc/rel7/soln/voip11/index.htm

The following steps refer to documents at the above website.

Step 2 Refer to the following online document at the *Cisco SS7 Interconnect for Voice Gateways Solution, Release 1.1* site:

Cisco Media Gateway Controller Hardware Installation Guide

Step 3 Refer to the following chapter in the *Cisco Media Gateway Controller Hardware Installation Guide*:

"Preparing the Installation Site"

Note the instructions that are specific to the hardware you have selected.

Step 4 Refer to the following chapter in the *Cisco Media Gateway Controller Hardware Installation Guide*:

"Hardware Installation Instructions"

a. Read the section "Installation Preview" in the above chapter, and note the instructions specific to the hardware you have selected.

b. Read the section “Installing the Cisco SLT” in the above chapter, and follow the instructions there.

c. Refer to the section “Installing and Configuring PCI Interface Cards” in the above chapter, and install the interface cards required for your network.

d. For further information on installing Cisco SLT interface cards and connecting to a network, refer to the *Cisco WAN Interface Cards Hardware Installation Guide*, at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/access/acs_mod/cis2600/hw_inst/wic_inst/wic_doc/index.htm

Step 5 Refer to the following chapter in the *Cisco Media Gateway Controller Hardware Installation Guide*:

“Cabling and Connections”

Connect your hardware components to the network as appropriate for your installation.

Step 6 Refer to the following chapter in the *Cisco Media Gateway Controller Hardware Installation Guide*:

“Power and Grounding”

Refer to the section “Connecting the Cisco SLT,” and ensure that you observe the appropriate power and grounding requirements.

Step 7 Refer to *Cisco SS7 Interconnect for Voice Gateways Solution, Release 1.1*, at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/access/sc/rel7/soln/voip11/index.htm

Step 8 Refer to the following online document at the *Cisco SS7 Interconnect for Voice Gateways Solution, Release 1.1* website:

Cisco Media Gateway Controller Software Release 7 Installation and Configuration Guide

Step 9 Refer to the following chapter in the *Cisco Media Gateway Controller Software Release 7 Installation and Configuration Guide*:

“Configuring the Cisco Signaling Link Terminal”

Read the section “Before Configuration” in the above chapter, with emphasis on the subsections “Prerequisites” and “Installing the Hardware.”

Installing Cisco SLT Software

To function as a Cisco SLT and terminate SS7 signaling links, the Cisco 2611 router must be running a special version of the Cisco IOS software. The Cisco SLT is shipped with this Cisco IOS software, but if you have an existing Cisco 2611, you must install the correct version. For the latest information, refer to the online release notes for the most recent version of the Cisco Media Gateway Controller (Signaling Controller) software.

Cisco SLT WAN Interface Cards and Cables

To support your network and traffic requirements, you can select from a variety of WAN interface cards (WICs) and voice/WAN interface cards (VWICs) to connect to the SS7 network.

About the T1/E1 Multiflex Trunk Interfaces

The T1/E1 multiflex trunk interface cards are dual-mode T1 or E1 interfaces in a VWIC (Voice/WAN Interface Card) form for voice, data, and integrated voice/data applications. They support the SS7 Cisco SLT function, as do serial WICs.

The T1/E1 VWIC supports the following T1/E1 functionality:

- Single or dual port, structured or unstructured T1/E1 functionality

- Drop and Insert (also called TDM Cross-Connect) between the T1/E1 ports on dual-port cards, used to hairpin bearer channels to a media gateway device and allowing the interchange of time-division multiplexing (TDM) slots between the ports on a two-port card
- Physical layer alarm forwarding feature between the two T1/E1 ports on dual-port cards

For additional information about the T1/E1 multiflex trunk interface cards, see *Cisco WAN Interface Cards Hardware Installation Guide* at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/access/acs_mod/cis2600/hw_inst/wic_inst/wic_doc/index.htm

Note For serial WICs, no particular configuration is required, except to ensure that the interfaces are not shut down.

For information about configuring other types of WICs, see *Cisco WAN Interface Cards Hardware Installation Guide*.

Table 5-2 lists the WAN interface cards, their part numbers, and the cable types required.

Table 5-3 Cisco SLT WAN Interface Cards and Cables

Card Type	Description	Product Number	Cable Type Required
VWIC	1-port T1 multiflex trunk interface	VWIC-1MFT-T1	T1/E1 cable with RJ-45 connector
	1-port E1 multiflex trunk interface	VWIC-1MFT-E1	
	2-port T1 multiflex trunk interface	VWIC-2MFT-T1	
	2-port E1 multiflex trunk interface	VWIC-2MFT-E1	
Drop and Insert[1] VWIC	2-port T1 multiflex trunk interface with drop and insert	VWIC-2MFT-T1-D1	
	2-port E1 multiflex trunk interface with drop and insert	VWIC-2MFT-E1-D1	
Serial WIC	1-port high-speed serial interface	WIC-1T	RS-449, RS-530, V.35
	2-port high-speed serial interface	WIC-2T	the above or blue “smart” cable

[1] Drop and Insert is another term for the TDM cross-connect function.

About Logical Channels

Each SS7 link defined on the SC is considered a logical channel, and each logical channel corresponds to a physical interface on the Cisco 2611. You can define two SS7 links (logical channels) from the SC to a Cisco 2600 series router. The logical channels map to the physical serial interfaces on the router from right to left, as follows:

- Numbering for an interface in the first slot always starts with channel 0.
- Numbering for an interface in the second slot always starts with channel 2.
- If a slot is empty, these rules still apply.

Table 5-4 shows some examples of how different signaling termination channels might map to physical interface positions on the Cisco 2611.

For more information about configuring the Signaling Controller software, see the documentation that came with it.

Table 5-4 Mapping of Logical Signaling Termination Channels to Cisco 2611 Interfaces

Logical Channel	Cisco 2611 Physical Interface			
	Two 2-Port WICs	**1-Port WIC on Right, 2-Port on Left**	**Two 2-Port WICs**	**2-Port WIC on Right, 1-Port on Left**
0	Not used: Serial 0/0	Assigned to port in first (right) slot: Serial 0/0	Not used: Serial 0/0	Not used: Serial 0/0
1	Assigned to second port in first (right) slot: Serial 0/1	—	Not used: Serial 0/1	Assigned to second port in first (right) slot: Serial 0/1
2	Not used: Serial 0/2	Assigned to first port in second (left) slot: Serial 0/1	Assigned to first port in second (left) slot: Serial 0/2	Assigned to first port in second (left) slot: Serial 0/2
3	Assigned to second port in second (left) slot: Serial 0/3	Not used: Serial 0/2	Assigned to second port in second (left) slot: Serial 0/3	—

Restrictions

Note the following restrictions on the interface cards:

- Only SS7 serial interfaces and protocols are supported. There is no support for HDLC, PPP, Frame Relay, ATM, X.25, or other non-SS7 serial WAN protocols.
- Each Cisco SLT supports only two SS7 signaling links.
- Each T1 or E1 port supports only one SS7 signaling link.

Although only two MTP 2 links can be terminated using the Cisco SLT, the two MTP 2 links can be terminated by using both ports of a 2-port VWIC/WIC, or two links can be terminated across two VWIC/WICs, one on each.

In addition to the WAN or dual-mode interface cards, the following minimum hardware is required:

- For 2T WICs, an individual cable from the following list is needed for each interface being used for link termination:
  - EIA/TIA-449: CAB-SS-449FC EIA/TIA-449 Cable, DCE Female to Smart Serial, 10 ft; CAB-SS-449MT EIA/TIA-449 Cable, DTE Male to Smart Serial, 10 ft
  - EIA/TIA-530: CAB-SS-530AMT EIA/TIA-530 Cable, DTE Male to Smart Serial, 10 ft (no female EIA/TIA-530 available)
  - V.35: CAB-SS-V35FC V.35 Cable, DCE Female to Smart Serial, 10 ft; CAB-SS-V35MT V.35 Cable, DTE Male to Smart Serial, 10 ft
- For 1T WICs, an individual cable from the following list is needed for each interface being used for link termination:
  - EIA/TIA-449: CAB-449MT EIA/TIA-449 Cable, DTE, Male, 10 ft; CAB-449FC EIA/TIA-449 Cable, DCE, Female, 10 ft
  - EIA/TIA-530: CAB-530MT EIA/TIA-530 Cable, DTE, Male, 10 ft (no female EIA/TIA-530 available)
  - V.35: CAB-V35MT V.35 Cable, DTE, Male, 10 ft; CAB-V35FC V.35 Cable, DCE, Female, 10 ft

- For a T1/E1 VWIC, a T1/E1 cable with RJ-45 connector is required.
- Cable connectors—EIA/TIA-449, EIA/TIA-530, V.35, and gender—depend upon your preference and requirements.
- The power source—48V DC or AC—depends on your preference and requirements.

Note After the Cisco SLT is configured, you must configure the point codes, linksets, SS7 signaling links, and the associated MTP 2 parameters on the signaling controller. See Create the File config.mml, page 5-10.

GLOSSARY

For terms or acronyms not listed below, see Internetworking Terms and Acronyms at the following URL:

http://www.cisco.com/univercd/cc/td/doc/cisintwk/ita/index.htm

A

AAA	authentication, authorization, and accounting
ALTDGK	alternate directory gatekeeper
AMA	automatic messaging accounting
ANI	automatic number identification
APC	adjacent point code
ARJ	authorization reject
ARP	authorization permit
ASP	application service provider
ARQ	authorization request

B

BHCA	busy hour call attempts

C

CAC	call admission control
CAS	channel-associated signaling
CCITT	Consultative Committee for International Telegraphy and Telephony
CCS	common-channel interoffice signaling
CDR	call detail record
CHAP	Challenge Handshake Authentication Protocol
CIC	Cisco Info Center; carrier identification code

CLI	command line interface
CO	central office
CSR	carier sensitive routing; customer service record
CVM	CiscoWorks2000 Voice Manager

D

DGK	directory gatekeeper
DHCP	Dynamic Host Configuration Protocol
DNIS	dialed number identification service
DPC	destination point code
DRQ	disconnect request
DTE	data termination equipment

E

EIA	Electronic Industry Alliance
EMEA	Europe, Middle East, and Africa
EMS	element management system
EO	end office
ETSI	European Telecommunications Standards Institute

F

FG	feature group

G

GK	gatekeeper
GKRCS	gatekeeper-routed call signaling

GKTMP	GateKeeper Transaction Message Protocol—a Cisco-proprietary protocol that allows third-party applications to influence the operation of the IOS GK
GW	gateway

H

HSRP	Hot Standby Router Protocol—used to ensure GK fault tolerance

I

IMT	intermachine trunk
IPM	Cisco’s Internetwork Performance Monitor
ISP	Internet service provider
ISUP	ISDN User Part
ITSP	Internet telephony service provider
ITU	International Telecommunication Union
IVR	interactive voice response
IXC	interexchange carrier—a regulated U.S. Class 4 carrier that is often a wholesale customer

L

LCF	location confirm
LCR	least-cost routing
LEC	local exchange carrier

M

MDO	message definition object
MGC	media gateway controller
MGCP	Media Gateway Control Protocol
MIB	management information base
MML	Man Machine Language

MSU	message signaling unit
MTP	message transfer protocol

N

NAS	network access server (gateway)
NI-2	National ISDN version 2—a BRI circuit
NMS	network management system
NFAS	Non-Facility Associated Signaling
NOA	nature of address
NOC	network operations center
NTP	Network Time Protocol

O

OLO	other licensed operator
OOS	out of service
OPC	origination point code
OSP	Open Settlements Protocol
OSS	operations support system
OPT	Open Packet Telephony

P

PDF	portable document format
PIN	personal identification number
POP	point of presence
PSTN	public switched telephone network
PTT	Post, Telephone, Telegraph—a government-mandated or -operated national telephony carrier

Q

QoS	quality of service

R

R2	A type of CAS used widely in places other than North America
RADIUS	Remote-Authentication Dial-In User Service
RAI	resource availability indicator
RAS	H.225 Registration, Admission, and Status Protocol—spoken between H.323 gateways and their gatekeepers
RCF	request confirm
RLM	redundant link manager
RRJ	request reject
RRQ	registration request
RTP	Realtime Transport Protocol
RTS	real-time server
RTSP	Real-Time Streaming Protocol— for controlling the streaming of RTP packets from a storage source
RUDP	Reliable User Datagram Protocol

S

SAA	service assurance agent
SC	signaling controller—a Cisco SC2200 signaling gateway that converts SS7 to a backhauled NI-2 protocol to gateways
SGCP	Simple Gateway Control Protocol
SLT	signaling link termination—a Cisco 2611 machine capable of terminating SS7 at the MTP2 layer and backhauling MTP3 (and up) to the SC2200 or virtual switch controller (VSC)
SNMP	Simple Network Management Protocol
SS7	Signaling System 7
SSL	secure socket layer

SSP	signaling service point
STC	signaling termination channel

T

TAC	Technical Assistance Center
TCL	Tool Command Language
TDM	time division multiplex
TFTP	Trivial File-Transfer Protocol
TIA	Telecommunications Industry Association
TIPHON	Telecommunications and Internet Protocol Harmonization Over Networks; commonly referred to as ETSI TIPHON (see ETSI)

U

URL	uniform resource locator
UDP	User Datagram Protocol
URQ	unregistration request

V

VSA	vendor-specific attribute—a nonstandard attribute tag used by RADIUS. Cisco has defined many useful VSAs to enhance the gateway CDR format.
VSC	virtual switch controller—one of various Cisco machines capable of providing SS7 signaling conversion, and able to control gateways by means of MGCP; referred to as the SC in this document
VWIC	Voice/WAN interface card

W

WIC	WAN interface card

INDEX