Cisco ASAP Solution 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

Customer Order Number:
Text Part Number: OL-1396-01

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.

CCIP, the Cisco *Powered* Network mark, the Cisco Systems Verified logo, Cisco Unity, Follow Me Browsing, FormShare, Internet Quotient, iQ Breakthrough, iQ Expertise, iQ FastTrack, the iQ Logo, iQ Net Readiness Scorecard, Networking Academy, ScriptShare, SMARTnet, TransPath, and Voice LAN are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, Discover All That's Possible, The Fastest Way to Increase Your Internet Quotient, and iQuick Study are service marks of Cisco Systems, Inc.; and Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, the Cisco IOS logo, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherSwitch, Fast Step, GigaStack, IOS, IP/TV, LightStream, MGX, MICA, the Networkers logo, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, RateMUX, Registrar, SlideCast, StrataView Plus, Stratm, SwitchProbe, TeleRouter, and VCO are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

All other trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0203R)

Cisco ASAP Solution Implementation Guide

CONTENTS

Preface xi

- Document Version and Solution Release xi
- Audience xii
- Scope xii
- Document Organization xii
- Related Documents xiii
  - Viewing Online Documents in Your Browser xiv
- Document Conventions xiv
- Terms and Acronyms xvi
- Obtaining Documentation xvi
  - World Wide Web xvi
  - Documentation CD-ROM xvi
  - Ordering Documentation xvi
  - Documentation Feedback xvii
- Obtaining Technical Assistance xvii
  - Cisco.com xvii
  - Technical Assistance Center xvii
    - Cisco TAC Web Site xviii
    - Cisco TAC Escalation Center xviii

CHAPTER 1 **Introduction** 1-1

- Basic Configurations 1-2
- Establishing Required and Optional Components 1-2

CHAPTER 2 **Configuring a Universal Gateway for Service** 2-1

- Basic Gateway Configuration 2-2
  - Baseline Configuration 2-2
  - Configuring Controllers 2-4
    - Configuring T1 and E1 Controllers 2-4
    - Configuring T3 Controllers 2-5
  - Configuring Network Timing 2-7
  - Configuring ISDN PRI on the Gateway (Optional) 2-7
  - Configuring Controllers for NFAS 2-8

Enabling SS7 Interconnect on the Gateway (Optional) 2-9

Defining the ISDN Switch Type 2-9

Configuring the ISDN Serial Interfaces 2-9

Configuring RLM 2-10

Using SS7 Interconnect References 2-11

Enabling Services 2-11

Enabling Dial Services 2-11

Configuring Dial-In (Asynchronous) Modem Service 2-12

Configuring ISDN Synchronous Service for Dial 2-13

Enabling Multichassis Multilink PPP 2-14

Enabling VPDN 2-15

Using Virtual Access Interfaces 2-17

Additional Optimization Techniques for Dial Services 2-17

Enabling Voice Services 2-17

Establishing Unified Dial Plans 2-17

Assigning Dial Peers to Voice Ports 2-18

Configuring H.323 Registration 2-19

Enabling Prepaid 2-20

Enabling T.38 Fax Relay Service 2-21

Enabling TDM Switching Services 2-22

Example TDM Switching Configuration 2-23

Enabling AAA and RADIUS 2-25

Enabling Basic AAA Service: Overview 2-25

Enabling Basic AAA Service: Examples 2-25

Enabling H.323-Based Accounting for Voice 2-25

A Basic AAA Example 2-26

Additional AAA Accounting Options 2-27

Other AAA Options 2-27

Administrative Options for AAA 2-28

Enabling Communications between a Gateway and a RADIUS Server 2-29

Enabling PPM 2-32

Enabling Local RPM 2-32

Establishing Resource Pools and VPDNs 2-32

Assigning Dial DNIS Groups to Support Local RPM (Optional) 2-33

Enabling Cisco RPMS on the Gateway 2-34

Enabling RADIUS-Based PPM 2-34

Enabling CAC 2-35

Enabling Call Treatment 2-35

Using Reporting Features 2-36

Enabling Reporting 2-36

Enabling Logging 2-37

Enabling SNMP on the Gateway 2-37

Configuring CallTracker 2-38

Optimizing the Universal Gateway 2-39

Optimizing CPU Efficiency 2-39

Maximizing CPU for Various Processes 2-40

Optimizing Port Resources 2-40

Optimizing System Logging 2-40

Disabling PPP Multilink Fragmentation 2-41

Preventing Process Takeover 2-41

Scaling AAA Processing 2-41

Optimizing Access Lists 2-41

Platform-Specific Considerations 2-42

Optimizing Modems 2-42

Managing Modem Recovery 2-42

Defining Basic Modem Capability 2-43

Suppressing Modem Startup Tests and Autotests 2-44

Optimizing SNMP 2-44

Using Virtual Access Interfaces to Optimize Dynamic Interface Configuration 2-45

Creating Virtual Access Interfaces Selectively 2-45

Precloning Virtual Access Interfaces 2-46

Additional General Recommendations 2-46

Delay Trunk Activation 2-46

Enable Passive Header Compression 2-46

Optimize Line Configuration for Dial Service 2-47

Special Topics 2-47

Enabling Modem Features: V.44 and V.92 2-47

V.44 Features 2-47

V.92 Features 2-47

Managing Echo Cancellation 2-48

Overview 2-48

Disabling Echo Cancellation 2-49

Changing Tail-Delay Coverage 2-49

Typical Echo-Cancellation Settings 2-50

UG and GK Configuration Requirements for Microsoft NetMeeting with T.38 Fax Relay 2-50

Configuring the NetMeeting Application 2-50

Configuring the UG for NetMeeting 2-51

Configuring the GK for NetMeeting 2-51

CHAPTER 3 Configuring Optional Network Components 3-1

Introduction 3-1

Establishing Additional Components to Support Dial 3-1

Establishing Additional Components to Support Voice 3-2

Provisioning SS7 Interconnect for Voice 3-2

Designing and Provisioning H.323 VoIP Networks 3-2

Establishing a Gatekeeper 3-3

Establishing a Directory Gatekeeper 3-4

Additional Server Support for Dial and Voice 3-4

CHAPTER 4 Using Management and Shared Support Services 4-1

Introduction 4-1

Resource and Network Management 4-2

Call Admission Control and RSVP 4-2

Basic Call Admission Control 4-3

Enhanced CAC Features 4-4

Resource Availability Indicator 4-4

Gateway Health Resources 4-5

Call Treatment 4-6

Call Rate Restriction 4-7

End-to-End Bandwidth 4-8

End-to-End Voice Quality 4-9

Additional QoS Remedies 4-11

IP Precedence 4-11

Low-Latency Queuing 4-11

RSVP/LLQ Integration 4-12

Link Fragmentation and Interleaving 4-12

Traffic Engineering Guidelines 4-13

Challenges with Low-Speed Links (<1.5 Mbps) 4-13

Packet Residency 4-13

Bandwidth Consumption 4-13

Other Bandwidth and Core Related Issues 4-14

Gateway with High-Speed Egress Interface 4-14

Gateway with Low-Speed Egress Interface 4-14

Edge Router with High-Speed Egress Interfaces 4-15

Edge Router with Low-Speed Egress Interfaces 4-15

Gateway with High-Speed Egress Interface 4-15

Core Issues 4-16

Optimizing the Performance of the Cisco SC2200 4-16

L2TP Tunneling and VPDNs 4-17
Before Configuring the LAC or LNS 4-18
Configuring VPDN on the LAC 4-18
Perform Global LAC Configuration 4-18
Edit LAC VPDN Parameters 4-19
Configuring VPDN on the LNS 4-20
Perform Global LNS Configuration 4-21
Edit LNS VPDN Parameters 4-22
Enabling Cisco RPMS 1.x 4-23
Overview 4-23
Required Activities 4-23
Optional Activities 4-24
Basic Configuration 4-24
Summary of Key Steps 4-29
Enabling VPDN (Optional) 4-29
Configuring SGBP (Optional) 4-29
An Example UG-to-RPMS Configuration 4-30
Useful Troubleshooting Commands 4-30
SS7 Resource Groups 4-31
An Example SS7 Resource Group 4-32
Enabling Cisco AR 4-32
Overview of Authentication and Authorization on the Cisco AR 4-33
Basic Authentication and Authorization 4-33
Using Cisco RLM 4-34
Configuring Multilink PPP 4-34
Multilink PPP 4-34
Multichassis Multilink PPP 4-34
Enabling SNMP 4-35
Using MIBs 4-35
Obtaining MIBs 4-36
Using MIB Locator 4-36
CHAPTER 5 Establishing Solution Components 5-1
Establishing H.323 Core Components 5-1
Gateways 5-1
Cisco AS5350 5-2
Cisco AS5400 5-2
Cisco AS5800 5-3
Cisco AS5850 5-3

Gatekeepers and Directory Gatekeepers 5-4
Cisco 3640, Cisco 3660 5-4
Cisco 7202 5-4
Cisco 7204 5-4
Cisco 7206 5-4
Establishing SS7 Signaling Components 5-4
Establishing Cisco Catalyst Switches 5-5
Establishing Management and Shared Support Services 5-5
Network Timing 5-5
L2TP Network Server 5-5
Cisco Universal Gateway Manager 5-6
CiscoWorks2000 Voice Manager 5-6
Cisco MGC Node Manager 5-6
Cisco Voice Services Provisioning Tool 5-6
Cisco Info Center 5-7
Cisco Internetwork Performance Monitor 5-7
Cisco Access Registrar 5-7
Cisco Resource Pool Manager Server 5-7
IVR Services 5-7
Billing Systems for Calling Card Services 5-8
APPENDIX A AAA Method Lists A-1
AAA Authentication Method Lists A-1
Authentication Services A-1
Types of Authentication Lists and Methods A-2
Order of Authentication Lists A-2
Authentication Syntax A-2
AAA Authorization Method Lists A-3
Authorization Services A-3
Types of Authorization Lists and Methods A-3
Order of Authorization Lists A-3
Authorization Syntax A-4
AAA Accounting Method Lists A-4
Accounting Services A-4
Types of Accounting Lists and Methods A-4
Order of Accounting Lists A-5
Accounting Syntax A-5

APPENDIX B Format C B-1

GLOSSARY

INDEX

Preface

The Cisco ASAP (Any Service, Any Port) Solution is a unified network architecture that delivers integrated data, voice, fax, and wireless services at a profit, serving both end users and application developers. Cisco AS5000 series universal gateways are the foundation of the network infrastructure. These platforms handle dial, VoIP, fax, and TDM switching services on a call-by-call basis. In addition, the Cisco ASAP Solution is compatible with the Cisco AS5300 and Cisco AS5800 where these are required to provide dial-only service.

This document and other documents related to this solution can be found under Cisco Any Service, Any Port (ASAP) Solution at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/access/solution/asap/index.htm

Note All Cisco solutions documents can be found under Cisco Solutions, at the following URL: http://www.cisco.com/univercd/cc/td/doc/solution/index.htm

This preface presents the following major topics:

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

Document Version and Solution Release

This is the first release of this document, which covers Release 1.0(0) of the Cisco ASAP Solution. Software upgrades or bug fixes to Release 2.0 will be indicated by 1.0(1), 1.0(2), and so on. As significant new features are added, the subsequent major releases will be indicated by 2.0(0), 3.0(0), and so on. Document version history is detailed below.

Document Version Number	Date	Notes
1	12/12/01	This document was first released.
2	04/03/02	Gateway provisioning has been expanded and made more modular. VPDN (L2TP) provisioning has been detailed.

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 CAS and PRI signaling on the Cisco AS5000 series
- Familiarity with configuring a basic H.323 gateway on the Cisco AS5000 series
- Familiarity with configuring a basic H.323 gatekeeper on the Cisco 3600 or 7200 series
- Familiarity with the following Cisco Solutions:
  - Cisco Wholesale Voice Solution
  - Cisco SS7 Interconnect for Voice Gateways Solution
  - Cisco SS7 Interconnect for Access Servers Solution

Note For documentation on all Cisco solutions, refer to Cisco Solutions at the following URL: http://www.cisco.com/univercd/cc/td/doc/solution/index.htm

Scope

This document presents the fundamental design and configuration information that is required to establish the various services provided by the Cisco ASAP 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 ASAP 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
Preface	Preface	Provides an overview of this document and lists related resources.

Chapter 1	Introduction	• Basic Configurations • Establishing Required and Optional Components
Chapter 2	Configuring a Universal Gateway for Service	• Basic Gateway Configuration • Enabling Services • Enabling AAA and RADIUS • Enabling PPM • Enabling CAC • Using Reporting Features • Optimizing the Universal Gateway • Special Topics
Chapter 3	Configuring Optional Network Components	• Establishing Additional Components to Support Dial • Establishing Additional Components to Support Voice • Additional Server Support for Dial and Voice
Chapter 4	Using Management and Shared Support Services	• Resource and Network Management • Additional QoS Remedies • Traffic Engineering Guidelines • Enabling Cisco RPMS 1.x • Enabling Cisco AR • Using Cisco RLM • Enabling SNMP
Chapter 5	Establishing Solution Components	• Establishing H.323 Core Components • Establishing SS7 Signaling Components • Establishing Cisco Catalyst Switches • Establishing Management and Shared Support Services
Glossary	Glossary	Defines abbreviated terms used in this document
Index	Index	

Related Documents

The majority of the documents referred to in the *Cisco ASAP Solution 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. 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. 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. Also used to represent variables in command line examples where `screen` font is used.
[ ]	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.

Note the 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 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 Means the following information *will help you solve a problem*. The tips information might not be troubleshooting or even an action, but could be useful information, similar to a Timesaver.

Terms and Acronyms

For definitions of terms and acronyms used in the following chapters, refer to the glossary at the end of this document.

For an online listing of internetworking terms and acronyms, refer to the following URL:

http://www.cisco.com/univercd/cc/td/doc/cisintwk/ita/index.htm

Obtaining Documentation

The following sections explain how to obtain documentation from Cisco Systems.

World Wide Web

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

http://www.cisco.com

Translated documentation is available at the following URL:

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

Documentation CD-ROM

Cisco documentation and additional literature are available in a Cisco Documentation CD-ROM package, which is shipped 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 through 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, elsewhere in North America, by calling 800 553-NETS (6387).

Documentation Feedback

If you are reading Cisco product documentation on Cisco.com, you can submit technical comments electronically. Click **Leave Feedback** at the bottom of the Cisco Documentation home page. After you complete the form, print it out and fax it to Cisco at 408 527-0730.

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:

Cisco Systems
Attn: Document Resource Connection
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 by using the Cisco Technical Assistance Center (TAC) Web Site. Cisco.com registered users have complete access to the technical support resources on the Cisco TAC Web Site.

Cisco.com

Cisco.com is the foundation of a suite of interactive, networked services that provides immediate, open access to Cisco information, networking solutions, services, programs, and resources at any time, from anywhere in the world.

Cisco.com is a highly integrated Internet application and a powerful, easy-to-use tool that provides a broad range of features and services to help you to

- Streamline business processes and improve productivity
- Resolve technical issues with online support
- Download and test software packages
- Order Cisco learning materials and merchandise
- Register for online skill assessment, training, and certification programs

You can self-register on Cisco.com to obtain customized information and service. To access Cisco.com, go to the following URL:

http://www.cisco.com

Technical Assistance Center

The Cisco TAC is available to all customers who need technical assistance with a Cisco product, technology, or solution. Two types of support are available through the Cisco TAC: the Cisco TAC Web Site and the Cisco TAC Escalation Center.

Inquiries to Cisco TAC are categorized according to the urgency of the issue:

- Priority level 4 (P4)—You need information or assistance concerning Cisco product capabilities, product installation, or basic product configuration.
- Priority level 3 (P3)—Your network performance is degraded. Network functionality is noticeably impaired, but most business operations continue.
- Priority level 2 (P2)—Your production network is severely degraded, affecting significant aspects of business operations. No workaround is available.
- Priority level 1 (P1)—Your production network is down, and a critical impact to business operations will occur if service is not restored quickly. No workaround is available.

Which Cisco TAC resource you choose is based on the priority of the problem and the conditions of service contracts, when applicable.

Cisco TAC Web Site

The Cisco TAC Web Site allows you to resolve P3 and P4 issues yourself, saving both cost and time. The site provides around-the-clock access to online tools, knowledge bases, and software. To access the Cisco TAC Web Site, go to the following URL:

http://www.cisco.com/tac

All customers, partners, and resellers who have a valid Cisco services contract have complete access to the technical support resources on the Cisco TAC Web Site. The Cisco TAC Web Site requires a Cisco.com login ID and password. If you have a valid service contract but do not have a login ID or password, go to the following URL to register:

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

If you cannot resolve your technical issues by using the Cisco TAC Web Site, and you are a Cisco.com registered user, you can open a case online by using the TAC Case Open tool at the following URL:

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

If you have Internet access, it is recommended that you open P3 and P4 cases through the Cisco TAC Web Site.

Cisco TAC Escalation Center

The Cisco TAC Escalation Center addresses issues that are classified as priority level 1 or priority level 2; these classifications are assigned when severe network degradation significantly impacts business operations. When you contact the TAC Escalation Center with a P1 or P2 problem, a Cisco TAC engineer will automatically open a case.

To obtain a directory of toll-free Cisco TAC telephone numbers for your country, go to the following URL:

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

Before calling, please check with your network operations center to determine the level of Cisco support services to which your company is entitled; for example, SMARTnet, SMARTnet Onsite, or Network Supported Accounts (NSA). In addition, please have available your service agreement number and your product serial number.

Introduction

The *Cisco ASAP Solution Implementation Guide* will help you establish, configure, and manage the services introduced in the *Cisco ASAP Solution Overview and Planning Guide*. Links to that and other documentation related to this solution are available at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/access/solution/asap/index.htm

The *Cisco ASAP Solution Overview and Planning Guide* introduces many factors that must be taken into account in designing a network that takes advantage of the capabilities of Cisco AS5000 series universal gateways (UGs). It is expected that you are familiar with that document.

This chapter briefly introduces and presents links for the following major topics:

- Basic Configurations
- Establishing Required and Optional Components

To summarize, the service scenarios supported by the Cisco ASAP Solution are as follows (refer to Chapter 2, “Solution Architecture and Services,” in the *Cisco ASAP Solution Overview and Planning Guide)*:

- Dial and Wireless Data
- PC to Phone
- Prepaid VoIP
- Phone to Phone
- Unified Communications
- TDM Switching
- T.38 Fax Relay

Note Only the fundamental steps to establish unified communications are listed in Table 2-1 of the *Cisco ASAP Solution Overview and Planning Guide*, to illustrate the basic issues. T.37 store-and-forward fax is not supported in initial releases of the Cisco ASAP Solution.

Begin by reviewing the requirements and issues associated with each service. Table 2-1 of the *Cisco ASAP Solution Overview and Planning Guide* lists the procedures required to implement each of these services.

Basic Configurations

Basic configurations are presented in the following chapters:

- Chapter 2, "Configuring a Universal Gateway for Service" presents the key issues of provisioning a universal gateway (UG) for basic service, and includes a variety of support options.
- Chapter 3, "Configuring Optional Network Components" presents configuration essentials related to such network options as SS7 interconnect and H.323 messaging.
- Chapter 4, "Using Management and Shared Support Services" discusses in detail the configuration issues related to optional applications.

Establishing Required and Optional Components

You may or may not already have the components needed to implement the majority of services provided by the Cisco ASAP Solution. Some of these are required, some are not. See Chapter 5, "Establishing Solution Components," for links to information about the following:

- Establishing H.323 Core Components

  Optional. Required for voice services in initial releases of the Cisco ASAP Solution, in the absence of SIP or MGCP support. Covers the following:

  - Gateways
  - Gatekeepers and Directory Gatekeepers

- Establishing SS7 Signaling Components

  Optional. Required where SS7 signaling must be accommodated. Covers the Cisco SC2200 platform and signaling link terminals (SLTs).

- Establishing Cisco Catalyst Switches

  Optional. Covers Cisco 6000 Family switches

- Establishing Management and Shared Support Services

  Optional and Required. Covers a variety of tools, both in the Cisco IOS and in stand-alone applications and components, including the following:

  - Network Timing
  - L2TP Network Server
  - Cisco Universal Gateway Manager
  - CiscoWorks2000 Voice Manager
  - Cisco MGC Node Manager
  - Cisco Voice Services Provisioning Tool
  - Cisco Info Center
  - Cisco Internetwork Performance Monitor
  - Cisco Access Registrar
  - Cisco Resource Pool Manager Server
  - IVR Services
  - Billing Systems for Calling Card Services

Note The above are introduced in Chapter 3, “Solution Components,” of the *Cisco ASAP Solution Overview and Planning Guide*.

CHAPTER 2

Configuring a Universal Gateway for Service

This chapter presents examples of configuring a universal gateway for service as part of the Cisco ASAP Solution. It also presents options for various scenarios, as well as recommendations to optimize performance.

Caution Certain features vary from one Cisco IOS release to another, as do configuration requirements. Before configuring a platform, always refer to the latest release notes for the solution. The release notes for the Cisco ASAP Solution are available at the following URL: http://www.cisco.com/univercd/cc/td/doc/product/access/solution/asap/index.htm

For configurations of other solution components, such as gatekeepers and supporting servers, see Chapter 3, "Configuring Optional Network Components."

Note The term *gateway* is used here generically to refer to a Cisco AS5000 series universal gateway (UG) access platform that supports the functions illustrated in this section. Although the term *gateway* has a specific meaning within the context of H.323 RAS signaling, this term is applicable even where optional H.323 is not used. Furthermore, traditionally when dial/modem services were referred to, the access platform supporting those services was referred to as a network access server, or NAS. The term *gateway* is used within the context of the Cisco ASAP Solution to describe an access platform providing the dial/modem function, as well as a single UG that is capable of functioning as both a NAS and a voice gateway.

Many of the following configuration and optimization topics are discussed in detail in Chapter 3, "Basic Configuration Using the Command-Line Interface," and Chapter 6, "Configuring Voice over IP," in *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/as5350/sw_conf/53swcg/

The following major topics are covered in this chapter:

- Basic Gateway Configuration
- Enabling Services
- Enabling AAA and RADIUS
- Enabling PPM
- Enabling CAC
- Using Reporting Features

- Optimizing the Universal Gateway
- Special Topics

Basic Gateway Configuration

This section presents the following fundamental topics and example configurations on the gateway:

- Baseline Configuration
- Configuring Controllers
- Configuring Network Timing
- Configuring ISDN PRI on the Gateway (Optional)
- Configuring Controllers for NFAS
- Enabling SS7 Interconnect on the Gateway (Optional)

Baseline Configuration

"Baseline" includes such universal issues as setting timestamps, establishing a time zone, establishing connections with TFTP servers, and the like. The following annotated configuration excerpt illustrates these issues.

Step 1 Enable timestamps, relative to the local time zone, for debugging and logging. Timestamps are required for logging messages to have meaning. (See also Enabling Logging, page 2-37.)

```
no service single-slot-reload-enable
no service pad
service timestamps debug datetime msec show-timezone
service timestamps log datetime msec show-timezone
service password-encryption

hostname <name>
```

Step 2 Ensure that testing is suppressed, and that console logging is disabled. See Suppressing Modem Startup Tests and Autotests, page 2-44, and Optimizing System Logging, page 2-40.

```
no boot startup-test

logging buffered 1000000 debugging
logging rate-limit console 10 except errors
no logging console guaranteed
no logging console
```

Caution Take care that excessive logging does not overwhelm the CPUs.

```
enable secret <secret>
!
username <name> password <password>
!
resource-pool disable
```

Step 3 Establish a time zone and other clock parameters.

```
clock timezone PDT -8
clock summer-time PDT recurring
clock calendar-valid
!
voice-fastpath enable
ip subnet-zero
no ip source-route
no ip gratuitous-arps
```

Step 4 Create a loopback interface, to ensure that operations are not dependent on a single physical interface being up. See Enabling Communications between a Gateway and a RADIUS Server, page 2-29.

```
interface Loopback0
 ip address <address subnet-mask>
 no ip mroute-cache
 no keepalive
```

Note A loopback interface can be used as a source address for many operations (routing protocols, group-async, RADIUS servers. In this case it corresponds to the source interface for TACACS+.

Step 5 Configure FastEthernet interfaces.

```
interface FastEthernet<interface>
 description <description>
 ip address <address subnet-mask>
 no ip mroute-cache
 load-interval 60
 duplex full
 speed 100
 no cdp enable
```

Step 6 Repeat the above for other FastEthernet interfaces as required.

Step 7 Establish an interface for TFTP server connections.

```
ip tftp source-interface <interface> no ip domain-lookup
!
no ip dhcp-client network-discovery
```

Step 8 Establish a fax interface. The following are defaults.

```
fax interface-type modem
mta receive maximum-recipients 0
```

Note The default for **interface-type** depends on the feature card configuration. If a modem is present, the default is **modem**, the case for universal port cards. For fax configuration information, refer to the following:

T.38 Fax for Cisco Universal Gateways at the following URL:
http://www.cisco.com/univercd/cc/td/doc/product/access/acs_serv/as5400/sw_conf/ios_121/puldtfax.htm

Fax Services at the following URL:
http://www.cisco.com/univercd/cc/td/doc/cisintwk/intsolns/voipsol/fax_isd.htm

The above reference also discusses the command **mta**, which sets options for SNMP Mail Transport Agents (MTAs).

```
ip classless
ip route 0.0.0.0 255.255.255.255 <default-gateway>
no ip http server
!
no cdp run
!
call rsvp-sync
!
voice-port <interface>:D <---see Note below
```

Note Voice port interfaces are created automatically when ISDN serial D-channels are created.

```
line con 0
 exec-timeout 60 0
 password 7 0300520A0A1B2C49
logging synchronous
line aux 0
 no exec
 logging synchronous
line vty 0 4
 exec-timeout 60 0
```

Configuring Controllers

References to resources, as well as examples, are provided below for T1, E1, and T3 (channelized T3, or CT3) controllers.

Configuring T1 and E1 Controllers

Fundamentals and References

For the fundamentals of configuring T1 and E1 controllers, refer to Configuring Channelized T1 and E1 Trunk Cards in Chapter 3, “Basic Configuration Using the Command-Line Interface,” in *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/as5350/sw_conf/53swcg/

For VoIP applications, refer to Configure Signaling on Voice Ports in Chapter 6, “Configuring Voice over IP,” in that document.

For a variety of examples of T1 and E1 controller configurations for VoIP, including PRI, refer to Chapter 4, “Provisioning Non-SS7-Based POPs” in the *Cisco Wholesale Voice Solution Design and Implementation Guide* at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/access/sc/rel7/soln/wv_rel1/wvpg/index.htm

The following configuration examples, although presented for a Cisco AS5300, are also applicable to UGs:

- E1 R2
- PRI ETSI
- PRI NI2
- T1 CAS FGB

- T1 CAS FGD

Example T1 Controller Configuration

The following example illustrates how to configure T1 controllers.

Step 1 Configure T1 controllers. See also Enabling TDM Switching Services, page 2-22.

```
controller T1 1/0
 framing esf
 linecode b8zs
```

Note The default framing is **sf**, and the associated default linecode is **ami**. This and the above framing and linecode are always paired.

Step 2 Repeat Step 1 for each additional T1 controller. For more details see Enabling SS7 Interconnect on the Gateway (Optional), page 2-9.

Note When NFAS (non-facility associated signaling) is implemented, multiple spans (controllers) will use the same D-channel (see Step 1).

Refer to Chapter 3, “Basic Configuration Using the Command-Line Interface,” of *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/as5350/sw_conf/53swcg/

Refer also to the following in that chapter: Configuring ISDN PRI, Configuring the D Channels for ISDN Signaling, and Configuring ISDN NFAS on CT1 PRI Groups.

Configuring T3 Controllers

Fundamentals and References

For the fundamentals of configuring T3 Controllers, refer to Configuring Channelized T3 Trunk Cards and Configuring ISDN PRI in Chapter 3, “Basic Configuration Using the Command-Line Interface,” in *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/as5350/sw_conf/53swcg/

The following configuration excerpt illustrates the essentials of configuring T3 controllers for PRI service, as well as other key features as noted. Variable options are indicated as follows: <option>.

Step 1 Configure a T3 controller. Framing and cable length will vary.

```
controller T3 1/0
 framing m23
 cablelength 20
 t1 1-28 controller
```

Step 2 Repeat the above for each additional T3 controller.

Note The numbering of steps in this example is for reference only, and generic provisioning not of interest to this solution is not commented on. The order in which various configurations are presented is not the order in which provisioning would occur. Furthermore, privileged EXEC mode is required to enter the commands resulting in the configurations illustrated below.

Step 1 Enable timestamps for debugging and logging.

```
no service single-slot-reload-enable
no service pad
service timestamps debug datetime msec show-timezone
service timestamps log datetime msec show-timezone
service password-encryption

hostname <name>
```

Step 2 Ensure that testing is suppressed, and that console logging is disabled. See Suppressing Modem Startup Tests and Autotests, page 2-44, and Optimizing System Logging, page 2-40.

```
no boot startup-test

logging buffered 1000000 debugging <---for logging lines, see Caution below
logging rate-limit console 10 except errors
no logging console guaranteed
no logging console
```

Caution Take care that excessive logging does not overwhelm the CPUs.

```
enable secret <secret>
!
username <name> password <password>
!
resource-pool disable
```

Step 3 Establish a time zone and other clock parameters.

```
clock timezone PDT -8
clock summer-time PDT recurring
clock calendar-valid
!
voice-fastpath enable
ip subnet-zero
no ip source-route
no ip gratuitous-arps
```

Step 4 Establish an interface for TFTP server connections.

```
ip tftp source-interface <interface> no ip domain-lookup
!
no ip dhcp-client network-discovery
!
fax interface-type modem
mta receive maximum-recipients 0
```

Step 5 Configure a T3 controller. Framing and cable length will vary. See Configuring T3 Controllers, page 2-5.

```
controller T3 1/0
 framing m23
 cablelength 20
 t1 1-28 controller
```

Configuring Network Timing

The NTP (Network Timing Protocol) clock period is automatically defined.

```
ntp clock-period 17179936 <---see Caution below
ntp update-calendar <---a recommended option
```

Caution Do not alter the default **clock-period** setting.

Step 1 To cause the system calendar to be updated periodically from the NTP time source, use the command **ntp update-calendar**.

Note For a discussion of NTP, refer to Enabling Management Protocols: NTP, SNMP, and Syslog at the following URL: http://www.cisco.com/univercd/cc/td/doc/cisintwk/intsolns/as5xipmo/sysmgt.htm

Step 2 Define a primary and a secondary NTP server.

```
ntp server 15.1.0.97
ntp server 16.1.0.109 prefer
```

Configuring ISDN PRI on the Gateway (Optional)

ISDN PRI may or may not be required in your network. The following is only an example. For the details of SS7 configuration, see Enabling SS7 Interconnect on the Gateway (Optional), page 2-9.

Step 1 Configure the serial interface. This is also required for NFAS signaling. See Configuring Controllers for NFAS, page 2-8.

```
interface Serial1/0:1:23
 no ip address
 no ip proxy-arp
no logging event link-status
 no keepalive
 no snmp trap link-status
 isdn switch-type primary-5ess
 isdn incoming-voice modem
 no fair-queue
 no cdp enable
```

Step 2 Establish the ISDN switch type of the telco service provider. See Enabling SS7 Interconnect on the Gateway (Optional), page 2-9, and Defining the ISDN Switch Type, page 2-9.

```
isdn switch-type <switch-type>
```

Note For a discussion of ISDN switch types, refer to National ISDN Switch Types for Basic Rate and Primary Rate Interfaces at the following URL: http://www.cisco.com/univercd/cc/td/doc/product/software/ios113ed/113t/113t_3/natisdn.htm

Caution Cisco recommends that you consult with your telephony service provider to ensure compatibility with the PSTN before proceeding. To support SS7 interconnect, a switch type of **primary-ni** is required. See Defining the ISDN Switch Type, page 2-9.

Note When a controller is configured for PRI, serial interfaces are created automatically. Repeat the above for each additional serial interface that is automatically created. See also Configuring the ISDN Serial Interfaces, page 2-9, for information specifically related to enabling synchronous dial services.

Step 3 Optimize the use of the ISDN B-channel.

```
isdn negotiate-bchan resend-setup
isdn bchan-number-order ascending <---important! see Caution below
```

Caution To reduce the chance of B-channel glare (assignment contention) with bidirectional traffic, make the near-end hunt proceed in a direction opposite that of the far-end setting. As the default is **descending**, it is probably the setting at the far end. However, take care to confirm the far-end hunt direction first.

Configuring Controllers for NFAS

This is optional for PRI, but is required for SS7 interconnect.

With NFAS (non-facility-associated signaling) multiple spans share the same D-channel. The D-channel configuration is on the interface associated with the primary NFAS controller. In this case, it is serial 1/0:1:23.

Step 1 Use the following general syntax to configure a controller for PRI NFAS:

```
controller <T1 | E1 controller ID>
 pri-group timeslots 1-24 nfas_d primary nfas_int <number> nfas_group <number>
```

Step 2 Configure, at a minimum, the following:

```
controller <T1 | E1 controller ID>
 pri-group timeslots 1-24 nfas_d primary nfas_int 0 nfas_group 0
controller <T1 | E1 controller ID>
 pri-group timeslots 1-24 nfas_d none nfas_int 1 nfas_group 0
```

Caution The NFAS interface number (nfas_int *number*) must be unique to each trunk (controller). All trunks must be placed in the same NFAS group (here *nfas_group 0)*.

Enabling SS7 Interconnect on the Gateway (Optional)

Support for SS7 signaling may or may not be required in your network. On the gateway, the basic configuration consists of the following activities:

- Defining the ISDN Switch Type
- Configuring the ISDN Serial Interfaces
- Configuring Controllers for NFAS
- Configuring RLM

Additional options can be configured. For more detail refer to Using SS7 Interconnect References, page 2-11.

Note Predefined SS7 resource groups are automatically created when resource pooling is enabled to a Cisco RPMS from a UG that is configured for SS7 interconnect. For details see SS7 Resource Groups, page 4-31.

Defining the ISDN Switch Type

SS7 signaling requires a PRI (primary) national ISDN (ni) switch type. Use the following global configuration command:

```
isdn switch-type primary-ni
```

Note The only switch type supported for SS7 interconnect is **primary-ni**.

Configuring the ISDN Serial Interfaces

ISDN serial interfaces require signaling that is out of band, over a dedicated data channel, the D-channel. The following configuration is on the D-channel interface (Serial1/0:1:23). [See Configuring ISDN PRI on the Gateway (Optional), page 2-7.]

Step 1 Configure the incoming D-channels for ISDN signaling. This is the D-channel defined previously in the NFAS configuration. See Configuring Controllers for NFAS, page 2-8.

Note Refer to Configuring the D Channels for ISDN Signaling in Chapter 3, “Basic Configuration Using the Command-Line Interface,” of *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/as5350/sw_conf/53swcg/

```
interface Serial1/0:1:23
 ip unnumbered Loopback0
 dialer idle-timeout 2147483
 no snmp trap link-status
 isdn incoming-voice modem
```

Note ISDN signaling is from the Cisco RLM. See Configuring RLM, page 2-10 and Using Cisco RLM, page 4-34.

```
 no isdn send-status-enquiry
 isdn negotiate-bchan resend-setup <---will negotiate for another B-channel if one is busy
 no fair-queue
```

Note For more information and references on multilink PPP and multichassis multilink PPP, see Configuring Multilink PPP, page 4-34.

Configuring RLM

Where SS7 interconnect is used, Redundant Link Manager (RLM) is a feature that provides virtual link management over multiple IP networks so that the Q.931 signaling protocol and other proprietary protocols can be transported on top of multiple redundant links between the Cisco Signaling Controller (in our case, the Cisco SC2200) and the gateway. In addition, RLM opens, maintains, and closes multiple links, manages buffers of queued signaling messages, and monitors whether links are active for link failover and signaling controller failover. The user can create more than one IP connection between the signaling control and the gateway.

Note The following deals with configuring RLM on the gateway only. See Using Cisco RLM, page 4-34. For more information about RLM, refer to Redundant Link Manager (RLM) at the following URL: http://www.cisco.com/univercd/cc/td/doc/product/access/acs_serv/as5400/sw_conf/ios_121/pull_rlm.htm

Configure RLM Groups

Use the following to establish an RLM group and server.

```
rlm group 0
 server <SC2200-reference>
 link address <SC2200-IP-address> source <interface> weight 1
```

The server name, *SC2200-reference*, only has local significance. The link IP address specified, *SC2200-IP-address*, is that of the Cisco SC2200. The source interface determines the source IP address that will be used by the gateway for RLM traffic.

Two RLM groups can be defined, allowing for redundant links to the Cisco SC2200; however, they must be defined with different **weight** values. The one with the higher weight is the primary group and is used unless it is out of service.

Note The interface defined (for example, Ethernet0) is that of the interface providing the connection to the signaling and management network, not that of the data network connection.

Specify the RLM Group Number

On the Serial0:23 interface (the D-channel), use the following to assign the **rlm-group** number that ISDN will start using.

```
interface Serial0:23
 isdn rlm-group 0
```

Note This ensures that the ISDN protocol stack functions properly while the D-channel information (Q.931 and the Q.921 frames) is transported over possibly multiple IP networks through UDP across links managed by the RLM. See also Configuring the ISDN Serial Interfaces, page 2-9.

For more details refer to ISDN Module at the following URL:
http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120t/120t3/isdn_123.htm

Using SS7 Interconnect References

For complete details of configuring SS7 interconnect, consult the SS7 interconnect solution documentation. References to SS7 interconnect for voice and dial services are presented below.

SS7 Interconnect for Voice Services

For the details of configuring SS7 on a gateway for voice services, refer to Configuring Media Gateways for the SS7 Interconnect for Voice Gateways Solution at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/access/sc/rel7/soln/voip13/gateway/dascfg5.htm

SS7 Interconnect for Dial Services

For the details of configuring SS7 on a gateway for dial (modem data) services, refer to Configuring Media Gateways for the SS7 Interconnect for Access Servers Solution at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/access/sc/rel7/soln/voip13/gateway/dascfg6.htm

The remainder of the SS7 configuration takes place on the components of the Cisco SC2200 node. See Establishing Additional Components to Support Dial, page 3-1.

Enabling Services

This section presents the following service-related topics:

- Enabling Dial Services
- Enabling Voice Services
- Enabling T.38 Fax Relay Service
- Enabling TDM Switching Services

Enabling Dial Services

Dial services fall into two fundamental categories, according to whether the data streams rely on a system clock or not: synchronous (ISDN) and asynchronous. Key configurations for each category, respectively, are presented in the following:

- Configuring Dial-In (Asynchronous) Modem Service
- Configuring ISDN Synchronous Service for Dial
- Enabling Multichassis Multilink PPP
- Enabling VPDN

- Using Virtual Access Interfaces
- Additional Optimization Techniques for Dial Services

Configuring Dial-In (Asynchronous) Modem Service

To support modem service for analog dial calls, an asynchronous group interface is required, as well as a range of asynchronous interfaces (lines) to be supported. Using an asynchronous group interface makes it easy to configure a large number of interfaces by allowing them to be cloned from a single managed copy. This can reduce the number of lines in the configuration, because each asynchronous group interface configuration can be replaced by at least one *group-async*.

Tip To assign the asynchronous interfaces to a group-async interface, view the running configuration to determine the number of asynchronous lines that need to be aggregated.

Note For details, refer to Configuring the Asynchronous Group Interface, in Chapter 3, “Basic Configuration Using the Command-Line Interface,” of *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/as5350/sw_conf/53swcg/

Do the following to configure dial-in modem service.

Step 1 Establish a group-async interface. This interface controls the characteristics of analog dial calls.

```
interface Group-Async0
 ip unnumbered Loopback0
 encapsulation ppp
 no ip mroute-cache
 dialer in-band
 dialer idle-timeout <seconds> <---see Note below
```

Note **dialer idle-timeout** defaults to a nonzero value.

```
 async mode interactive <---see Note below
```

Note **async mode interactive** is required only if both EXEC and non-EXEC sessions are to be supported.

```
 no snmp trap link-status
 no peer default ip address
 ppp authentication chap callin <---CHAP options can vary
 group-range <start> <end> <---see Note below
```

Note A noncontiguous range of slots for the DSPs can be entered in the range and the software will adjust accordingly.

Step 2 Configure lines (support the dial-in interfaces). Configuring lines requires defining a range.

```
line <start> <end>
 exec-timeout 5 0
 no flush-at-activation
 modem InOut <---see Note below
```

Note If the gateway is being used *only* for dial-in services and COT support is not required, use **modem dialin** and **transport input none**.

Modem capability is defined automatically when the IOS detects the modems.

```
transport input all <---see Note above
 autoselect during-login <---see Note below
 autoselect ppp
```

Note The use of **autoselect during-login** is required only if both EXEC and non-EXEC sessions are to be supported.

Configuring ISDN Synchronous Service for Dial

To configure a synchronous dial service, first configure a synchronous dial (“Dialer”) interface, then associate a dialer interface group with a serial interface, as shown below.

Step 1 Configure a dialer interface.

```
interface Dialer1
 ip address negotiated
 encapsulation ppp <---see Caution below
 no ip route-cache
 no ip mroute-cache
 load-interval 60 <---see first Note below
 dialer in-band
 dialer idle-timeout <seconds>
dialer pool 1 <---see second Note below
 autodetect encapsulation ppp
 no peer default ip address
 no fair-queue
 no cdp enable
 ppp authentication chap callin
```

Note The command **load-interval** determines how often, in seconds, the traffic load is examined with respect to bringing up additional multilink PPP links when they are needed. This command is used only for dial-out services.

Note The **dialer pool 1** (above) must be associated with **dialer pool-member 1** (below) on the serial interface. The older method used **dialer-group 1**.

Caution The command **encapsulation ppp** is recommended for an ISDN synchronous data call. Of special importance on a UG is the statement **ppp multilink**, which is required to enable multilink PPP. (See also Enabling Multichassis Multilink PPP., below.) In addition, the command **isdn negotiate-bchan**

resend-setup is recommended for two-way TDM calls. By negotiating for another B-channel if a given channel is occupied, this prevents calls from being rejected. For more detail, see Enabling TDM Switching Services, page 2-22.

Step 2 Associate the dialer interface group just established with a serial interface.

```
interface Serial <number>
dialer pool-member 1 <---see Note below
```

Note The **dialer pool-member** is associated with **dialer pool 1**. The older method used **dialer rotary-group 1**.

Step 3 Repeat Step 1 and Step 2 for all serial interfaces that are to be associated with the dialer interface group.

Enabling Multichassis Multilink PPP

ISDN multichassis multilink PPP (MMP) is useful where there are large pools of dial-in users and a single chassis cannot provide enough dial ports. MMP uses Stack Group Bidding Protocol (SGBP) to enable MMP. (See Configuring SGBP (Optional), page 4-29.)

Note For background and provisioning information, refer to Layer 2 Tunnel Protocol at the following URL: http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120t/120t1/l2tpt.htm

Note For more background and detailed references on Multilink PPP (MLP) and Multichassis Multilink PPP (MMP), see Configuring Multilink PPP, page 4-34.

Use the following commands to enable SGBP to support MMP (Multichassis Multilink PPP) connections. See Configuring SGBP (Optional), page 4-29.

```
sgbp group sgbp1
sgbp member <hostname IP-address>
```

In this simple example with a stack that consists of two UGs, **sgbp member** defines the name and address of the partner UG. That UG would use this command to define the name and address of the current UG. Therefore, an **sgbp member** line must include all members of the stack with which the current UG must communicate.

Note The above information is very basic. For more information and references on multilink PPP and multichassis multilink PPP, see Configuring Multilink PPP, page 4-34.

Step 4 To enable SGBP, you must enable VPDN. See Enabling VPDN, below.

Enabling VPDN

Generically, an L2TP tunnel is referred to as a VPN (virtual private network) tunnel.

Note When L2F is used, the tunnel endpoint is called an HGW (home gateway). When L2TP is used, the tunnel endpoint is called an LNS (L2TP network server). The point of access to the network (in our case the UG) is often referred to as an LAC (L2TP access concentrator).

For an overview and details of configuring virtual private networks, refer to the chapter “Configuring Virtual Private Networks” in the *Cisco IOS Dial Technologies Configuration Guide, Release 12.2,* at the following URL:
http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fdial_c/index.htm

The establishment of VPDN groups is optional, and is an optimization techniques that employs *virtual templates* to speed the establishment of call interfaces.For background and information on how to complete this optional provisioning, see Using Virtual Access Interfaces to Optimize Dynamic Interface Configuration, page 2-45.

The following illustrates the establishment of *local* VPDN groups.

Note The gateway provisioning supports interactions with a Cisco RPMS. For details of Cisco RPMS, refer to Cisco Resource Pool Manager Server 1.1 at the following URL:
http://www.cisco.com/univercd/cc/td/doc/product/access/acs_soft/rpms/rpms_1-1/index.htm

(Later versions of Cisco RPMS are known as Cisco Resource Policy Management Server.)

See also L2TP Tunneling and VPDNs, page 4-17 and L2TP Network Server, page 5-5.

There are three basic types of VPDN:

- Local VPDN
- Remote (Server-Based) VPDN
- Cisco RPMS VPDN

Configuration issues related to these VPDN types are discussed in the sections that follow.

Note If you are using an LNS as the remote server, before proceeding see L2TP Tunneling and VPDNs, page 4-17. That section illustrates both gateway and server configurations.

Local VPDN

Use the following basic steps to configure VPDN manually on the gateway. If using an LNS, see Configuring VPDN on the LAC, page 4-18. See also Assigning Dial DNIS Groups to Support Local RPM (Optional), page 2-33.

Note For an overview and details of configuring virtual private networks, refer to the chapter “Configuring Virtual Private Networks” in the Cisco IOS Dial Technologies Configuration Guide, Release 12.2, at the following URL:
http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fdial_c/index.htm

Step 1 Enable VPDN, and tell the gateway to look for tunnel definitions.

```
vpdn enable
```

Note This is the only command required when VPDN definitions are server-based. Continue with the following basic steps if doing local VPDN.

Step 2 Define a local group number identifier for which other VPDN variables can be assigned. Valid range is from 1 through 3000.

```
vpdn-group <group-number>
```

Step 3 Enable the router to request a dial-in tunnel to an IP address, if the dial-in user belongs to a specific domain or dials a specific DNIS.

Note The following configuration example is *local* VPDN (VPN) information only. When Cisco RPMS or Cisco AR are running and have the appropriate VPDN information, the UG obtains its VPDN information from those applications. Therefore, a configuration on the UG (other than **vpdn enable**) is unnecessary.

```
vpdn enable
!
vpdn-group 23
 request-dialin
  protocol l2tp
  dnis Local_rpm_vispt
 initiate-to ip 10.120.5.20
 local name local_rpm_tid
 l2tp tunnel password 7 00071A150754
!
vpdn-group 31
 request-dialin
  protocol l2tp
  dnis Local_rpm_rispt
 initiate-to ip 10.130.5.20
 local name local_rpm_rispt
 l2tp tunnel password 7 0822455D0A16
```

Remote (Server-Based) VPDN

VPDN must also be enabled on a remote server, such as a Cisco RPMS or Cisco AR. See Configuring VPDN on the LNS, page 4-20.

Cisco RPMS VPDN

The details of configuring a UG to interact with a Cisco RPMS server are presented in Enabling Cisco RPMS 1.x, page 4-23.

Using Virtual Access Interfaces

Virtual access interfaces are logical entities that can optimize the dynamic configuration of serial interfaces for dial services. For the details of configuring this optimization technique, see Using Virtual Access Interfaces to Optimize Dynamic Interface Configuration, page 2-45.

Additional Optimization Techniques for Dial Services

The following sections present optimization techniques that are of value for dial services:

- Enable Passive Header Compression, page 2-46
- Optimize Line Configuration for Dial Service, page 2-47

Enabling Voice Services

After controllers are configured, the next essential step to enabling voice services is to configure a dial plan. Where universal ports are concerned, a *unified dial plan* is called for. This section presents the following topics:

- Establishing Unified Dial Plans
- Assigning Dial Peers to Voice Ports
- Configuring H.323 Registration

Establishing Unified Dial Plans

A unified dial plan is simply a dial plan that supports both voice and dial numbers. In a converged voice and dial network, a unified dial plan defines how any call, whether voice or dial, should be handled, including whether it should be terminated locally, routed across the network, processed by another element, and so on. This overall unified dial plan is typically implemented on a range of network elements that may include gateways, gatekeepers, route servers, proxy servers, and the like.

The gateway is the main element affected when implementing a unified dial plan (as opposed to a voice-only dial plan), because this is where the decision takes place as to whether or not a call should be processed locally as a dial call. Different called numbers are required to differentiate voice calls from dial calls.

The gateway dial plan implementation continues to define how the gateway should handle all incoming calls, including whether to terminate the call locally, initiate a script to play IVR prompts, forward the call to another gateway, use H.323 RAS (Registration Admission, and Status) messaging, and so on. In a unified dial plan implementation, this is extended to accommodate dial calls that the service provider wishes to have terminated locally.

Caution Currently, support for a unified dial plan is implemented through a feature commonly referred to as “fall through to dial.” T*here must be no matching dial peer for a dial access number if that number is to be handled as a dial call.*

Note For a discussion of dial plans in the context of voice services, refer to Dial Plans and Number Normalization in Chapter 2, “Provisioning the Gatekeeper Core” in the Cisco Wholesale Voice Solution Design and Implementation Guide at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/access/sc/rel7/soln/wv_rel1/wvpg/index.htm

The topic of static dial plans is discussed in even greater detail in Designing a Static Dial Plan at the following URL:
http://www.cisco.com/univercd/cc/td/doc/cisintwk/intsolns/voipsol/dp3_isd.htm

These are illustrated in the example configuration excerpts that follow.

Assigning Dial Peers to Voice Ports

The following configuration excerpts illustrate assigning dial peers to the voice ports of an H.323 gateway.

Step 1 Assign dial peers to voice ports using the following general syntax. Here we use an entire FastEthernet interface, and define both POTS and VoIP ports.

```
interface FastEthernet<interface>
h323-gateway voip interface
!
dial-peer voice <number> pots
 incoming called-number <area-code>
 direct-inward-dial
!
dial-peer voice <number> voip
 destination-pattern <area-code>
 session target ipv4:15.0.0.1
!
gateway
```

Note Subsequent steps provide the details of specific dial-peer configurations: POTS, VoIP, and prepaid. The voice ports that are shown are assigned automatically.

Caution Applications that are not compliant with T.38 Fax Relay, such as Microsoft NetMeeting, may not work properly unless certain configurations are applied to the dial peer as well as to the gatekeeper. For details see UG and GK Configuration Requirements for Microsoft NetMeeting with T.38 Fax Relay, page 2-50.

Step 2 Configure a POTS voice dial peer.

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

dial-peer voice 901 pots
 incoming called-number 902.......
 no shutdown
 destination-pattern 901110[0-4]...
 direct-inward-dial
 port 1/0:1:D
 prefix 901
```

Step 3 Configure a variety of VoIP dial peers.

```
dial-peer voice 903 voip
 destination-pattern 903.......
 session target ras <---forwards call to H.323 gatekeeper for RAS admission
!
```

```
dial-peer voice 9021092 voip
destination-pattern 9021092...
 session target ras
!
dial-peer voice 9021090 voip
destination-pattern 9021090...
 session target ras
 codec g711ulaw

dial-peer voice 901103 voip
 destination-pattern 901103....
 session target ras
```

Note For a discussion of **direct-inward-dial** and **session target ras**, refer to the technical note Voice–Understanding How Inbound and Outbound Dial Peers are Matched on Cisco IOS Platforms at the following URL:
http://www.cisco.com/warp/public/788/voip/in_dial_peer_match.html

Step 4 Configure a dial peer for prepaid calling-card services.

```
dial-peer voice 69 pots
 description ASAP_voice Prepaid
 application debit
 incoming called-number 8006661234
 destination-pattern 8006661234
 port 1/0:1:D
```

Note For a discussion of other aspects of enabling prepaid services for voice, see Enabling Prepaid, page 2-20.

Configuring H.323 Registration

The following discusses the configuration required to enable H.323 registration on a gateway so that the GW can register with a GK. For a discussion of what is required on the GK, see Establishing a Gatekeeper, page 3-3.

Step 1 Configure the UG to register with the GK.

Note Refer to Configuring Gateways and a Gatekeeper in a Single Zone, in Chapter 2, “Provisioning the Gatekeeper Core,” of the *Cisco Wholesale Voice Solution Design and Implementation Guide*, at the following URL:
http://www.cisco.com/univercd/cc/td/doc/product/access/sc/rel7/soln/wv_rel1/wvpg/index.htm

```
interface FastEthernet0/0
 ip address 10.40.4.4 255.255.0.0
 no ip directed-broadcast
 duplex full
 speed 100
 h323-gateway voip interface
 h323-gateway voip id z1-gk1 ipaddr 10.40.7.50 1718
 h323-gateway voip h323-id z1-gw3
 h323-gateway voip tech-prefix 1#
```

Enabling Prepaid

Enabling prepaid billing services for voice calls is discussed in considerable detail in Establishing Billing Services for Calling Card Services, in Chapter 3, “Provisioning Shared Support Services,” of the *Cisco Wholesale Voice Solution Design and Implementation Guide*, at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/access/sc/rel7/soln/wv_rel1/wvpg/index.htm

In addition to establishing a dial peer dedicated to this service, call treatment will need to be enabled and interactive voice response (IVR) facilities will need to be established and provisioned. The following fundamental steps are required:

- Configure Dial Peers for Prepaid
- Enable IVR
- Enable Accounting for Prepaid

Configure Dial Peers for Prepaid

An example dial peer for prepaid service is illustrated in Step 4 of Assigning Dial Peers to Voice Ports, page 2-18.

Enable IVR

Do something similar to the following to enable interactive voice response (IVR) prompts for prepaid calling-card services.

Note Refer to Provisioning Services to Support IVR in Chapter 3, “Provisioning Shared Support Services,” of the *Cisco Wholesale Voice Solution Design and Implementation Guide*, at the following URL: http://www.cisco.com/univercd/cc/td/doc/product/access/sc/rel7/soln/wv_rel1/wvpg/index.htm

Step 1 Declare the location of the Cisco TCL IVR scripts on a TFTP server.

```
call application voice debit tftp://10.100.10.10/tcl/app_debitcard.2.0.0.tcl
```

Step 2 Determine a user ID length.

```
call application voice debit uid-len 4
```

Step 3 In our example, make English the first language of choice.

```
call application voice debit language 1 en
```

Step 4 In our example, make Spanish the second language.

```
call application voice debit language 2 sp
```

Step 5 Declare the location of the two prompt files, respectively.

```
call application voice debit set-location en 0 tftp://10.100.10.10/prompts/en/
call application voice debit set-location sp 0 tftp://10.100.10.10/prompts/sp/
```

Enable Accounting for Prepaid

You will also need to enable H.323-based accounting on the gateway, an AAA feature. See Enabling H.323-Based Accounting for Voice, page 2-25.

Enabling T.38 Fax Relay Service

Cisco AS5350 and AS5400 UGs support fax over IP services in addition to VoIP. The Cisco T.38 Fax Relay for Universal Gateways feature provides standards-based fax relay protocol support on UGs.

Caution Applications that are not compliant with T.38 Fax Relay, such as Microsoft NetMeeting, may not work properly unless certain configurations are applied to the dial peer as well as to the gatekeeper. For details see UG and GK Configuration Requirements for Microsoft NetMeeting with T.38 Fax Relay, page 2-50.

Step 1 Enable T.38 Fax Relay service.

Note For more detail, see Enabling T.38 Fax Relay Service, page 2-21. Refer also to T.38 Fax for Cisco Universal Gateways at the following URL:
http://www.cisco.com/univercd/cc/td/doc/product/access/acs_serv/as5400/sw_conf/ios_121/puldtfax.htm

```
voice service voip
 fax protocol t38 ls-redundancy 0 hs-redundancy 0
!
fax interface-type vfc
```

Caution With certain PC telephony applications that are not T.38 compliant (for example, Microsoft NetMeeting), the global use of this command can be problematic. Cisco recommends that you disable T.38 Fax Relay on the VoIP dial peers that service such applications.

When a fax is sent from an originating GW, an initial voice call is established. The terminating GW detects the fax tone generated by the answering fax machine. The VoIP H.323 call stack then starts a T.38 mode request, using H.245 procedures. (H.245 is a core component of the H.323 standard that specifies messages for opening and closing channels for media streams, and other commands, requests and indications.) If the opposite end of the call acknowledges the T.38 mode request, the initial audio channel is closed and a T.38 Fax Relay channel is opened. When the fax transmission is completed, the call reverts back to voice mode.

The command **voice service voip** enters the voice service configuration mode. The subsequent command **fax protocol** specifies the global default fax protocol for all the VoIP dial peers. The keyword **t38** specifies the T.38 Fax Relay protocol.

Caution T.38 Fax Relay can be configured under **dial-peer voice**, but the configuration for the specific dial peer takes precedence over the global configuration implemented under **voice service voip**.

Note For further details, additional references, and configuration examples, refer to T.38 Fax Relay for Cisco Universal Gateways, at the following URL:
http://www.cisco.com/univercd/cc/td/doc/product/access/acs_serv/as5400/sw_conf/ios_121/puldtfax.htm

Enabling TDM Switching Services

After receiving an incoming call with SS7, ISDN PRI, or CAS signaling, Cisco UGs analyze the dialed digits and, if required, forward the call outward (using the appropriate outbound signaling) to the designated port or trunk group. This feature, variously referred to as “grooming,” “drop and insert,” or (in EMEA) “tromboning,” is necessary for PSTN interconnects to provide not only legacy voice services but also test calls. The TDM switching feature of the UGs allow cross-connections to be made directly on the time slot interchange (TSI) portion of the DSP.

Note TDM switching, the ability of Cisco AS5000 series UGs to switch information directly between two DS0 circuits without affecting the data, is introduced in TDM Switching, in Chapter 2, “Solution Architecture and Services,” of the *Cisco ASAP Solution Overview and Planning Guide* at the following URL:
http://www.cisco.com/univercd/cc/td/doc/product/access/solution/asap/overview/index.htm

Any Cisco AS5000 series trunk interface (T1 or E1, including T1s inside a CT3) can be designated as an outbound or inbound trunk for TDM switching purposes. SS7, network-side ISDN PRI, user-side ISDN PRI, or CAS signaling is provided on this outbound trunk to signal calls redirected by the UG. Calls to be redirected are identified simply through a dial-peer match of the called number, or DNIS (Dialed Number Identification Service).

Note Dial peers are discussed in TDM Switching, in Chapter 2, “Solution Architecture and Services,” of the *Cisco ASAP Solution Overview and Planning Guide* at the following URL:
http://www.cisco.com/univercd/cc/td/doc/product/access/solution/asap/overview/index.htm

See also Establishing Unified Dial Plans, page 2-17.

Refer also to the following useful documents at their respective URLs:

Configuring Voice over IP

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

Network Side ISDN PRI Signalling, Trunking, and Switching

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

Example TDM Switching Configuration

The example configuration presented below illustrates one way to configure both SS7-to-PRI and PRI-to-SS7 switching. Controllers 1/0:1 through 1/0:14 represent SS7 ingress and egress facilities. Controllers 1/0:15 through 1/0:28 represent ISDN non-NFAS ingress and egress facilities, with a switch type of NI2 (National ISDN-2).

In this example, any incoming SS7 10-digit call with the called-number NPA-NXX digits 904-102 is switched to the ISDN PRIs on controllers 1.0:15 through 1/0:28. Conversely, any incoming 10-digit call on the ISDN PRIs with the called-number NPA-NXX digits 904-704 is switched to the SS7 RLM NFAS group 0, which consists of controllers 1/0:1 through 1/0:14.

On the ISDN PRI egress side, this configuration provides two principal benefits:

- It uses dial-peer hunting to group a large number of T1 ISDN PRI spans into a single hunt group.
- It minimizes B-channel glare when TDM switched calls are processed in both directions, by using B-channel negotiation and opposing B-channel hunt schemes.

In the following excerpt, the first five steps simply configure the controllers. The last step, the configuration of dial peers, is what really enables TDM switching.

Step 1 Configure dial peers. This begins the actual TDM switching configuration.

```
dial-peer voice 1 pots
 description SS7 to PRI TDM switching <---see Note below
```

Note This dial peer begins the SS7-to-PRI hunt. By default its preference is 0, but there is no **preference 0** line.

```
 incoming called-number 904102.... <---periods represent wildcards
 destination-pattern 904102....
 no digit-strip
 direct-inward-dial
 port 1/0:15:D
 forward-digits all
!
dial-peer voice 2 pots <---second peer in the hunt, with preference 1
 description SS7 to PRI TDM switching
 preference 1
 incoming called-number 904102....
 destination-pattern 904102....
 no digit-strip
 direct-inward-dial
 port 1/0:27:D
 forward-digits all
!
dial-peer voice 3 pots <---third peer in the hunt, with preference 2
 description SS7 to PRI TDM switching
 preference 2
 incoming called-number 904102....
 destination-pattern 904102....
 no digit-strip
 direct-inward-dial
 port 1/0:16:D
 forward-digits all
!
<---snip---> dial-peers 4 through 9 not shown

dial-peer voice 10 pots <---tenth peer in the hunt, with preference 9
 description SS7 to PRI TDM switching
 preference 9
 incoming called-number 904102....
 destination-pattern 904102....
 no digit-strip
 direct-inward-dial
 port 1/0:23:D
 forward-digits all
!
dial-peer voice 11 pots <---eleventh peer in the hunt, with preference 10
 description SS7 to PRI TDM switching
 preference 10
 incoming called-number 904102....
 destination-pattern 904102....
 no digit-strip
 direct-inward-dial
 port 1/0:24:D
 forward-digits all
!
dial-peer voice 12 pots <---see Note below
```

Note This dial peer does not have a preference. It switches calls from the ISDN PRIs to the SS7 T1 controllers 1/0:1 through 1/0:14.

```
 description PRI to SS7 TDM switching peer
 incoming called-number 904704....
 destination-pattern 904704....
 no digit-strip
 direct-inward-dial
 port 1/0:1:D
 forward-digits all
```

Step 2 Configure B-channel negotiation to support simultaneous ingress and egress traffic. This is done on the serial controller that supports the SS7 D-channel, as in the following abbreviated example.

```
interface Serial1/0:1:23
 isdn negotiate-bchan resend-setup   <---important
```

Step 3 Reduce the chance of B-channel glare (assignment contention) with bidirectional traffic. To do this, make the near-end hunt proceed in a direction opposite that of the far-end setting.

Caution Take care to confirm the far-end hunt direction first.

Note the following abbreviated example.

```
interface Serial1/0:15:23
  isdn bchan-number-order ascending <---important
```

As the default is **descending**, it is probably the setting at the far end.

Enabling AAA and RADIUS

This section covers the following topics:

- Enabling Basic AAA Service: Overview
- Enabling Basic AAA Service: Examples
- Enabling Communications between a Gateway and a RADIUS Server

Enabling Basic AAA Service: Overview

Enabling basic AAA service consists of three fundamental steps:

1. Enabling AAA
2. Defining AAA servers
3. Defining *methods* to apply to each of the three elements of AAA: authentication, authorization, and accounting. This step requires the use of *method lists*, which will vary according to the needs of each network.

For background, the AAA method lists for authentication, authorization, and accounting are discussed in Appendix A, "AAA Method Lists."

Enabling Basic AAA Service: Examples

The following examples illustrate how to enable AAA accounting for voice services on the gateway. The following topics are covered:

- Enabling H.323-Based Accounting for Voice
- A Basic AAA Example
- Additional AAA Accounting Options
- Other AAA Options
- Administrative Options for AAA

Enabling H.323-Based Accounting for Voice

For prepaid services (see Enabling Prepaid, page 2-20, you will need to enable H.323-based accounting on the gateway. The **vsa** (vendor-specific attributes) command option is required to support prepaid voice services only.

```
gw-accounting h323 vsa <---required for prepaid service only
gw-accounting voip
```

Note For a discussion of VSAs in the context of AAA billing, refer to Understanding and Provisioning AAA Billing in Chapter 3, "Provisioning Shared Support Services," of the *Cisco Wholesale Voice Solution Design and Implementation Guide*, at the following URL:
http://www.cisco.com/univercd/cc/td/doc/product/access/sc/rel7/soln/wv_rel1/wvpg/index.htm

Refer in particular to Methods to Enable VoIP Accounting on Gateways to Support Billing in that section.

A Basic AAA Example

The following steps illustrate basic AAA provisioning. (There are many options that are beyond the scope of the current discussion.)

Step 1 Enable AAA.

```
aaa new-model
```

Step 2 Define AAA servers.

Typically AAA groups are used. This allows different servers to be used for each element of AAA. It also defines a redundant set of servers for each element. However, the keywords **radius** or **tacacs+** are also used. The latter approach uses globally defined RADIUS or TACACS+ servers, and is not as flexible as using AAA server groups.

a. Define a RADIUS AAA server.

```
aaa group server radius <server-group-name>
 server <IP-address/hostname> auth-port 1645 acct-port 1646
```

Note The above port numbers are defaults, for authorization and accounting, respectively. Explicit port numbers are required only if nondefault ports are used.

b. Alternatively, define a TACACS+ AAA server.

```
aaa group server tacacs+ <server-group-name>
 server <IP-address/hostname>
```

Step 3 Define AAA method lists. The following lines are processed sequentially.

a. Define an authentication method list.

```
aaa authentication login default local group <server-group-name>
```

Note For background on this and the other method lists, see Appendix A, “AAA Method Lists.”

This does the following. By default, authenticate users requesting login access by first checking the local username list. If the username is not listed locally, authentication will be through the AAA servers defined in the AAA group *server-group-name*. Defining local authentication first is typical where ports are being used by scripted login clients who use generic passwords (such as AOL). If there is no response from the servers, login users will not be able to access the network.

```
aaa authentication ppp default if-needed local group <server-group-name>
```

This does the following. By default, authenticate users requesting PPP access only if they have not already been authenticated. Authenticate first through the local database. If that fails, authenticate through the AAA servers defined in the group *server-group-name*. This can be used to access the gateway locally for administrative purposes in case, for example, network connectivity to the gateway is down.

b. Define an authorization method list.

```
aaa authorization exec default group server-group-name if-authenticated
```

This does the following. By default, authorize users running EXEC shells through the AAA servers defined in the AAA group *server-group-name*. If there is no response from the servers (for example, they are not working), just let them run the required services.

```
aaa authorization network default group server-group-name if-authenticated
```

c. Configure an accounting method list.

```
aaa accounting exec default start-stop group <server-group-name>
aaa accounting network default start-stop group <server-group-name>
```

Additional AAA Accounting Options

You can also define additional AAA accounting options. Select only those steps you want to apply. (The following commands are used in global configuration mode.)

Step 1 Ignore null usernames. This prevents the Cisco IOS software from sending accounting records for users whose username string is null.

```
aaa accounting suppress null-username
```

This prevents accounting packets from being sent for users who are autoselected as connecting through PPP. Initially the gateway assumes a login session (rather than a PPP session, which is aborted when PPP is detected).

Step 2 Include the IP address in the start record.

```
aaa accounting delay-start
```

Step 3 Send accounting records on system start/stop.

```
aaa accounting system default wait-start group <server-group-name>
```

As in start-stop, this sends both a start and a stop accounting notice to the accounting server. However, if you use the wait-start keyword, the requested user service does not begin until the start accounting notice is acknowledged. A stop accounting notice is also sent.

Other AAA Options

You may also find one or more of the following useful. (The following commands are used in global configuration mode.)

Step 1 To support RADIUS, use extended NAS port format (also applicable to UGs). The regular **nas port** attribute is still sent, but an accounting VSA is also sent with the extended NAS port information.

```
aaa nas port extended
```

This allows interfaces in the same slot to be differentiated (for example, 1/0:1 from 1/0:3).

Caution The above requires VSAs, so these must be enabled. See Enabling H.323-Based Accounting for Voice, page 2-25.

Step 2 Use multithreaded AAA processing. [This is required only in IOS releases prior to Cisco IOS Release 12.2(2)XB.]

```
aaa processes <n>
```

where *n* = the number of AAA processes.

Cisco recommends 5 < *n* < 15 for RADIUS-only environments, and 10 < *n* < 30 for environments with TACACS+.

Caution Adjust *n* with care, as this creates a bell-curve performance profile that is environment-specific. Increase its value to decrease the PPP queue, and ensure that the CPU is not burdened by PPP queue improvements.

Tip Use **show ppp queue** to check for improvements. For an example of CPU monitoring, see Scaling AAA Processing, page 2-41.

Administrative Options for AAA

Through the use of administrative *listnames*, you can control authentication, authorization, and accounting for administrative groups. Here we use the example listname ADMIN. Select only those steps you wish to apply. These options can be applied to console (**line con 0**), auxiliary (**line aux 0**), and virtual terminal (**line vty 0 4**) interfaces.

Step 1 Set login authentication on an interface. Here we define the listname.

```
login authentication ADMIN
```

Step 2 Define an administrative authentication method list.

```
aaa authentication login ADMIN group LAB local
```

This first authenticates users through the AAA server group LAB, then proceeds to the local username list. The AAA group ADMIN corresponds to the login authentication ADMIN configured in the previous step.

Step 3 Define an administrative authorization method list.

```
aaa authorization exec ADMIN group LAB if-authenticated
```

Note This does the following. The result is the same as for the previous command, but for the listname ADMIN, through the AAA servers defined in the AAA group LAB.

Step 4 Define an administrative command level for authorization.

```
aaa authorization commands level ADMIN group LAB if-authenticated
```

This does the following. The variable *level* is the specific command level that should be authorized. Valid entries are 0 through 15. Level 1 is normal user EXEC commands. Level 15 is the privileged level. There are five commands associated with privilege level 0: **disable**, **enable**, **exit**, **help**, and **logout**. If you configure AAA authorization for a privilege level greater than 0, these five commands will not be included in the privilege level command set.

Step 5 Configure an administrative accounting method list.

```
aaa accounting exec ADMIN wait-start group LAB
```

Step 6 Run accounting for all commands at the specified privilege level.

```
aaa accounting commands level ADMIN wait-start group LAB
```

This does the following. The variable *level* is the specific command level that should be tracked. Valid entries are 0 through 15. Level 1 is normal user EXEC commands. Level 15 is the privileged level. There are five commands associated with privilege level 0: **disable**, **enable**, **exit**, **help**, and **logout**. If you configure AAA authorization for a privilege level greater than 0, these five commands will not be included in the privilege level command set.

Note For details, refer to Accounting Commands at the following URL:
http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/12cgcr/secur_r/srprt1/sracct.htm

Step 7 Provide information about all outbound connections made from the gateway (such as Telnet, local-area transport (LAT), TN3270, packet assembler/disassembler, and rlogin).

```
aaa accounting connection ADMIN wait-start group LAB
```

Enabling Communications between a Gateway and a RADIUS Server

After AAA is enabled and RADIUS servers and keys are defined on the client gateway, communications must be established between the gateway and the RADIUS server. This section addresses the recommended configurations on the gateway, with the basic options you should configure there. See also Enabling RADIUS-Based PPM, page 2-34.

Caution You must enable AAA on the gateway before you can configure RADIUS. See Enabling Basic AAA Service: Examples, page 2-25.

Note A detailed discussion is also provided in Configure Communication between the Gateway and the RADIUS Server in Configuring a Gateway for AAA, Chapter 3, “Provisioning Shared Support Services,” of the *Cisco Wholesale Voice Solution Design and Implementation Guide*, at the following URL:
http://www.cisco.com/univercd/cc/td/doc/product/access/sc/rel7/soln/wv_rel1/wvpg/index.htm

The above-referenced section also illustrates how to configure the gateway to use VSAs and how to configure gateway-specific accounting.

The full RADIUS command syntax on the gateway is as follows:

```
radius-server host <IP-address/hostname> auth-port <number> acct-port <number>
[non-standard] timeout <seconds> retransmit <number> key <string>
```

Caution The order of option entry is important, as certain options are no longer available after you enter certain other options. Specifically, the key must be entered at the end.

Note Refer also to RADIUS Commands at the following URL:
http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122sup/122csum/csum2/122cssec/ssfrad.htm

There are many other options that are not addressed here. For a discussion of server implementations of RADIUS, 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

Do the following to establish communications. You can selectively define the parameters to override, and leave others at their default values by not defining them. (You cannot define **deadtime** as a server-specific parameter.)

Step 1 Define RADIUS servers, source address, authorization and accounting ports, and keys.

```
radius-server host <IP-address/hostname> auth-port <number> acct-port <number> key
<string>
```

The above line is required for each RADIUS server listed in an AAA server group. Define on the client gateway the authentication and accounting ports on the RADIUS server. These are the ports on the server to which the client will send authentication and accounting data. Keys are typically defined for each RADIUS server, although a global command is available. There is no default key.

Caution You will not be able to configure these ports after the key is established.

The Cisco defaults for **auth-port** and **acct-port** are 1645 and 1646, respectively. (The RFCs define these as 1812 and 1813, respectively.) The important thing is to make sure the client ports match the corresponding ports on the RADIUS server. Server-specific values must be defined as part of the **radius-server** definition for that server.

Step 2 Define additional communications parameters. These include timeouts, retries, and deadtime, as defined in the substeps below. The values shown in the configuration lines are Cisco's recommendations.

a. Define how many times the client should try to contact the server before giving up. (The default value is 3 retries.)

```
radius-server retransmit 2
```

b. Define how long the client should wait before retrying to get a response from the server. (The default value is 3 seconds.)

```
radius-server timeout 1
```

c. Define how long the client should wait before attempting to contact the server again. (This is the default.)

```
radius-server deadtime 1
```

This means that, after the RADIUS server is declared dead, the client will wait 1 minute before attempting to communicate with the server again.

Step 3 Define basic RADIUS server attributes. The following are Cisco's recommendations.

a. Distinguish EXEC from PPP sessions.

```
radius-server attribute 6 on-for-login-auth
```

This causes the client to send attribute 6 (Service-Type) set to “1” (login) for users connecting through EXEC, and to “2” for users connecting through PPP.

b. Send session IDs in all RADIUS packets.

```
radius-server attribute 44 include-in-access-req
```

The Accounting Session ID is a unique identifier used to calculate the session context. It is the only identifier provided by the RADIUS protocol that can relate authentication and accounting requests to one another with absolute certainty. Attribute 44 allows the service provider to track all RADIUS information associated with a specific call, from initial connection through termination. This is useful where preauthentication or VPDN is used.

c. If using a management and accounting built around Ascend’s port format (Format C), configure the RADIUS server to send Attribute 25 information and use Format C.

```
radius-server attribute 25 nas-port format c
```

Note Attribute 25 is not a VSA, but instead is an IETF *Class* attribute. The above string is typically included in the *access-accept* packet. If it is provided, it must also be included by the UG in *accounting-start* and *accounting-stop* packets.

Format C applies only if you are using the Ascend port format. For more information, see Appendix B, “Format C.” Otherwise, you can use any suitable format.

Step 4 Define additional RADIUS options. The following are Cisco’s recommendations.

a. Assign unique accounting session IDs.

```
radius-server unique-ident <number>
```

The above prepends a value defined to the Acct-Session-Id string. Each time the system reboots, this value increments and is updated in the system configuration.

For example, for

```
radius-server unique-ident 1
```

we initially have

```
acct-session-id = 01000008
```

Following a system reboot, we have

```
acct-session-id = 02000008
```

b. Enable vendor-specific attributes (VSAs). These are required for the client to send, receive, and process VSAs. The following lines enable VSAs for accounting and authentication, respectively.

```
radius-server vsa send accounting
radius-server vsa send authentication
```

VSAs are needed to support other options such as **aaa nas-port extended**. In this case both the accounting and authentication attributes are included, and the extended information is included in a VSA that is sent within Attribute 26.

Caution If **radius-server vsa send authentication** is enabled, depending on how the RADIUS server is configured, the server may echo back the attributes it received. If the client does not expect the VSA in the Access-Accept packet, it may drop the call.

c. To force RADIUS to use the IP address of a specified interface for all outgoing RADIUS packets

```
ip radius source-interface <interface>
```

Use this command to set a subinterface's IP address to be used as the source address for all outgoing RADIUS packets. This address is used as long as the interface is in the up state. In this way, the RADIUS server can use one IP address entry for every network access client instead of maintaining a list of IP addresses.

This ensures that the source IP address used for RADIUS packets from the client is deterministic. Typically, a loopback interface ensures that there is no dependence on a single physical interface being up.

Tip The above command is especially useful in cases where the router has many interfaces and you want to ensure that all RADIUS packets from a specific router have the same IP address.

Enabling PPM

This section discusses how to enable port policy management (PPM) on the gateway. PPM is not required, but is recommended wherever traffic and resources need to be managed. PPM can be enabled locally through RPM features, or it an be enabled remotely in conjunction with a Cisco RPMS or a RADIUS server.

This section presents the following basic topics:

- Enabling Local RPM
- Enabling RADIUS-Based PPM

Enabling Local RPM

Enabling RPM locally, on the client gateway, requires the following steps:

- Establishing Resource Pools and VPDNs
- Assigning Dial DNIS Groups to Support Local RPM (Optional)
- Enabling Cisco RPMS on the Gateway

Establishing Resource Pools and VPDNs

The following configuration excerpts illustrate the establishment of resource pools on the gateway (that is, for local RPM). The VPDNs are optional.

Step 1 Enable resource pools.

```
resource-pool enable
resource-pool call treatment resource channel-not-available
resource-pool call treatment profile busy
!
```

Step 2 The following illustrates the establishment of *local* VPDN (virtual private data network) groups. See Enabling Multichassis Multilink PPP, page 2-14, and Enabling VPDN (Optional), page 4-29.

Note The establishment of VPDN groups is optional. For details of Cisco RPMS, refer to Cisco Resource Pool Manager Server 1.1 at the following URL:
http://www.cisco.com/univercd/cc/td/doc/product/access/acs_soft/rpms/rpms_1-1/index.htm

VPDN groups contain the data required to build a VPDN (VPN) tunnel from the UG to the LNS. See also L2TP Tunneling and VPDNs, page 4-17 and L2TP Network Server, page 5-5.

Note For additional details see Resource Pool Management at the following URL:
http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120t/120t5/rpm1205t.htm

```
resource-pool profile vpdn Local_rpm <---arbitrary name
 limit base-size all
 limit overflow-size 0
!
resource-pool profile customer Local_rpm
 limit base-size 30
 limit overflow-size 10
 dnis group Local_rpm_rispt
 dnis group Local_rpm_vispt
 vpdn group 23
 vpdn group 31
 vpdn profile Local_rpm
```

Step 3 Establish a resource pool profile with AAA parameters.

```
resource-pool profile customer Cisco_Customer
 limit base-size 30
 limit overflow-size 10
 dnis group DNIS_LIST1 <---see Note below
 dnis group DNIS_LIST2
 vpdn profile LOCAL_RPM
resource-pool aaa accounting ppp
resource-pool aaa protocol group tacacs+ local
```

Note See Assigning Dial DNIS Groups to Support Local RPM (Optional), page 2-33.

Assigning Dial DNIS Groups to Support Local RPM (Optional)

Resource pool management (RPM) allows wholesalers to aggregate dial resources across multiple gateways and allocate subsets of those resources to their retail ISP customers. RPM enforces service level agreements (SLAs) for dial access for each ISP. Where a better use of dial resources is required, a Cisco RPMS can be used.

The following illustrates local RPM only. To use a Cisco RPMS, see Enabling Cisco RPMS 1.x, page 4-23.

Step 1 Assign dial DNIS groups to support local RPM.

Note Refer to Configuring Media Gateways for the SS7 Interconnect for Voice Gateways Solution at the following URL:
http://www.cisco.com/univercd/cc/td/doc/product/access/sc/rel7/soln/das22/gateway/dascfg5.htm

```
dialer dnis group Local_rpm <---group names are arbitrary
!
dialer dnis group Local_rpm_rispt
 number 9011105008
!
dialer dnis group Local_rpm_vispt
 number 9011105007
```

Enabling Cisco RPMS on the Gateway

For a detailed illustration of enabling Cisco RPMS on the gateway, see Enabling Cisco RPMS 1.x, page 4-23.

Enabling RADIUS-Based PPM

Enabling RADIUS-based PPM consists essentially of establishing communications between the host gateway and one or more RADIUS servers, and enabling AAA preauthentication. Preauthentication can be specified according to the following criteria: CLID (Calling Line IDentification) number, call type, or DNIS number. You can also specify a group of DNIS numbers that will be bypassed for preauthentication.

Step 1 Ensure that communications are established between the gateway and a RADIUS server. See Enabling Communications between a Gateway and a RADIUS Server, page 2-29.

Step 2 Ensure that AAA is enabled. See A Basic AAA Example, page 2-26.

Step 3 To enter AAA preauthentication configuration mode, enter the following in global configuration mode:

```
Router(config)# aaa preauth
```

Step 4 The prompt changes. To specify a AAA RADIUS server group to use for preauthentication, enter the following at the prompt:

```
Router(config-preauth)# group <server-group>
```

Step 5 Specify preauthentication criteria as needed.

Note For details, refer to “Configuring AAA Preauthentication” in Configuring RADIUS at the following URL:
http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fsecur_c/fsecsp/scfrad.htm

Step 6 There is another method to configure DNIS preauthentication. For details, refer to the section mentioned in the previous note.

Step 7 In addition to configuring preauthentication on the gateway, you must also configure preauthentication profiles on a RADIUS server. For details, refer to the section mentioned in the previous note.

Enabling CAC

Call admission control, or CAC, is a feature that gracefully prevents call from entering the gateway if certain resources (for example, CPU capacity, memory, and interfaces) are not available to process those calls. To deal with high CPU use, large call volumes, or occasional large numbers of calls (spikes), CAC allows you to address both call spikes and call thresholds. Configure call spikes to limit the number of incoming calls over a short period of time. Configure call thresholds to define the circumstances under which system resources should be enabled.

For the details of CAC features, both basic and enhanced, see Call Admission Control and RSVP, page 4-2.

Caution Managing call spikes and thresholds is especially important in handling transactions involving debit cards, which require AAA and similar types of support.

Note For additional information on CAC, refer to Call Admission Control for H.323 VoIP Gateways at the following URL:
http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122limit/122x/122xa/122xa_2/ft_pfavb.htm

Enabling Call Treatment

The following steps illustrate the use of call treatment to establish a call threshold and a resource threshold. See Call Admission Control and RSVP, page 4-2. Both RAI (Resource Allocation Indicator) and non-RAI examples are shown.

Step 1 Enable call treatment. This example does not use RAI.

```
call treatment on <---enables call treatment
call threshold global cpu-5sec low 50 high 75 <---sets thresholds
call rsvp-sync
```

Note The above does not use RAI (Resource Allocation Indicators). Not all Call Admission Control (CAC) features are available in early releases of the Cisco ASAP Solution.

Step 2 Globally set a CAC H.323 RAI resource threshold on all ports. This also causes RAI information to be sent to the GK.

```
call threshold global cpu-avg low 90 high 95 busyout
gateway
 resource threshold high 90 low 85
```

Note See also Call Admission Control and RSVP, page 4-2. This topic was introduced in Chapter 5, "Solution Management," of the Cisco ASAP Solution Overview and Planning Guide.

Caution The above values should be appropriate for most situations. However, an issue related to ISDN cause codes must be taken into account. A cause code is sent after the high call threshold is crossed and the channels are in the process of transitioning from an IS (in-service) busy or IS idle state to an OOS (out-of-service) state. Before the channels go into an OOS state (which can take seconds to occur), any TDM call that attempts to connect to these channels will be rejected with a cause code of 41 (temporary failure).

Using Reporting Features

To be managed properly, networks of any considerable size require the collection of various types of data. This section discusses the fundamentals of reporting (including logging, syslog, and SNMP), as well as of the Cisco IOS feature known as CallTracker, under the following topics, respectively:

- Enabling Reporting
- Configuring CallTracker

Enabling Reporting

The details of enabling such reporting features as logging, syslog, and SNMP are covered in section 7, Enabling Management Protocols, of the Cisco AS5x00 Case Study for Basic IP Modem Services at the following URL:

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

The discussion there is applicable to gateways in general. The following example addresses syslog logging.

Cisco IOS software can send syslog messages to one or more element manager servers. Syslog messages are then collected by a standard UNIX or NT type syslog daemon. With syslog you can 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 a real-time scenario.
- Reserve telnet sessions for making configurations changes and using show commands. This prevents telnet sessions from getting cluttered up with debug output.

Syslog is recommended for all but the smallest networks. For syslog to be used, logging must first be enabled.

Caution To enable syslog, ensure that *console* logging is disabled. Use **show logging** to confirm this, and **no logging console** to turn off console logging if it is enabled.

After timestamps are enabled (see Baseline Configuration, page 2-2), there are two more fundamental steps to enabling reporting:

- Enabling Logging
- Enabling SNMP on the Gateway

Enabling Logging

Logging can be enabled by itself on the gateway, and is required for syslog to be used. Do the following to enable basic logging.

Step 1 Allow logging up to the debug level (all 8 levels) for all messages to be sent to a syslog server.

```
logging trap debugging
```

Step 2 If you are working with multiple gateways, assign a different logging facility tag to each server.

```
logging facility <facility-tag> <---for example, local4
```

Step 3 Assign the interface to the syslog server.

```
logging <source-interface> <---for example, FastEthernet0/1
```

Step 4 Assign the address of the syslog server.

```
logging <IP-address>
```

Enabling SNMP on the Gateway

The SNMP (Simple Network Management Protocol) traps generated by the gateway can provide a variety of useful information. This section is concerned only with what is required on the UG to enable SNMP. An SNMP server must also be configured. For more information see Enabling SNMP, page 4-35.

Caution Cisco recommends that you enable SNMP on all gateways. 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** (read only), and the management applications will take care of the rest.

Do the following to enable SNMP on the UG. The following example presents just a few options.

Step 1 Specify an SNMP server engine name (ID). Here we configure a local name.

```
snmp-server engineID local 80000009030000014280B352
```

Step 2 Define the community access string. Here it is public but read-only.

```
snmp-server community public RO
```

Step 3 Enable SNMP traps. Here we enable traps for ISDN at layer 2.

```
snmp-server enable traps isdn layer2
```

Note Refer also to Configuring Simple Network Management Protocol (SNMP) at the following URL:
http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/fun_c/fcprt3/fcd301.htm

Configuring CallTracker

CallTracker is a network management subsystem within the Cisco IOS. Relying on syslog and SNMP, CallTracker enables the tracking of calls and their attributes, from the ingress ports (T1, E1, CT3) to the DSP resource used. This feature captures detailed statistics on the status and progress of active calls and retains historical data for disconnected call sessions. CallTracker collects session information such as call states and resources, traffic statistics, total bytes transmitted and received, user IP address, and disconnect reason. The resulting database tables can be accessed through SNMP, syslog, or the Cisco IOS command line interface.

The primary purpose of CallTracker is not only to provide detailed output about the gateway's performance (such as the number of good vs. bad calls), but also to help improve the analysis and use of resources—for example, in determining which DSPs are not functioning properly, or which ingress channels are not in use.

Note CallTracker has many features that are not discussed here. CallTracker was originally introduced on Cisco AS5300 and AS5800 platforms, and is documented in greater detail in CallTracker plus ISDN and AAA Enhancements for the Cisco AS5300 and Cisco AS5800 at the following URL:
http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t3/dt_cltrk.htm

The following steps provide the basic operation of CallTracker on the gateway. You will also need to ensure that syslog and SNMP are enabled. See Enabling Reporting, page 2-36.

Step 1 Enable CallTracker.

```
calltracker enable
```

Step 2 Send call information to syslog for processing at a later date.

```
calltracker call-record <terse | verbose> [quiet]
```

By default, call record logging is disabled. Cisco recommends the options **verbose** and **quiet**. The subcommand **terse** generates a *brief set* of call records containing a subset of the data stored within CallTracker (used primarily to manage calls). The subcommand **verbose** generates a *complete set* of call records containing all of the data stored within CallTracker (used primarily to debug calls). The option **quiet** causes call records to be sent only a configured syslog server, and not to the console.

Step 3 Configure the history buffer.

Caution CallTracker does not report to the syslog server immediately after a call has disconnected. This is because it is not a high-priority process, and must wait for sufficient CPU capability to be available. This can take up to a minute. Consequently, the history buffer needs to be large enough to hold the data before reporting.

The syntax is as follows:

```
calltracker history max-size <number>
```

As a rule of thumb, figure out the maximum number of calls you will receive over a 1-minute period. Consider call length, call type, and the fact that ISDN calls are shorter than modem calls. Also consider that a configuration error or hardware failure in one part of the system could force a higher call rate in another part.

As a first estimate for *number*, Cisco recommends you begin with

number of ports on gateway x 4

where 4 takes into account 4 calls per second arriving on a gateway.

Step 4 Configure polling intervals for modem statistics. The syntax is as follows:

```
modem link-info poll time <seconds>
```

Cisco recommends 320 seconds.

The above sets the polling interval at which link statistics for disconnected calls are retrieved from the modem. As mentioned previously, this information is buffered and sent to the syslog server for later processing.

Optimizing the Universal Gateway

This section presents a variety of Cisco recommendations that will reduce processing overhead, logging interactions, and other system activities that can impair networks of any substantial size and traffic burden if they are not managed carefully. The following topics are presented:

- Optimizing CPU Efficiency
- Optimizing Modems
- Optimizing SNMP
- Using Virtual Access Interfaces to Optimize Dynamic Interface Configuration
- Additional General Recommendations

Note Some of these issues have already been addressed previously in this chapter. They are presented again here for convenience and emphasis.

Optimizing CPU Efficiency

Overburdening the processing power of a CPU can have a pronounced effect on overall network efficiency. The more overburdened CPUs there are in a network, the greater the impairment. This section discusses a variety of techniques to relieve the CPU of unnecessary tasks and allow it to deal with demanding ones as needed. The following topics are presented:

- Maximizing CPU for Various Processes
- Optimizing Port Resources
- Optimizing System Logging
- Disabling PPP Multilink Fragmentation

- Preventing Process Takeover
- Scaling AAA Processing
- Optimizing Access Lists
- Platform-Specific Considerations

Maximizing CPU for Various Processes

Processes such as ISDN Layer 2, EXEC sessions, AAA messaging, and the like must not be starved for CPU. Use one or both of the following terminal configuration commands to ensure that processing power is available for those processes:

Step 1 Determine the scheduling of low-priority processes.

```
scheduler interval 500
```

The above allows low-priority processes to be scheduled every 500 ms, thereby allowing some commands to be typed even if CPU use is at 100%.

Step 2 Guarantee CPU time for low-priority processes.

```
scheduler alloc 3000 1000
```

The above guarantees CPU time for low-priority processes by putting a maximum time allocated to fast switching (3000 ms) and process switching (1000 ms) for each instance of network interruption.

Note The above recommendations are found in Troubleshooting Router Hangs at the following URL: http://www.cisco.com/warp/public/63/why_hang.html

Optimizing Port Resources

To ensure that resources are available, you can use the following command to specify the percentage of available port resources required to enable a trunk line. (See Delay Trunk Activation, page 2-46.)

```
trunk activate port-threshold <percent>
```

Optimizing System Logging

Unnecessary logging can place unneeded burdens on platform CPUs. Logging to the console, in particular, can have undesired effects. Cisco recommends the following logging settings.

Step 1 Disable console logging. This is important, and the second command ensures it.

```
no logging console
no logging console guaranteed
```

Caution A failure to disable console logging can cause CPU interrupts, dropped packets, and denial of service events. The router might also lock up.

Step 2 In case you ever need to enable console logging, use the following **rate-limit** command option to prevent the console from being overwhelmed by messages:

```
logging rate-limit console 10 except errors
```

Step 3 Disable logging on serial D-channel interfaces and group async interfaces.

```
no logging event link-status
```

Step 4 Double-check features that generate logging. (See Configuring CallTracker, page 2-38.)

```
calltracker call-record terse quiet
```

Disabling PPP Multilink Fragmentation

PPP multilink fragmentation is enabled by default. Turning it off can relieve the load on the CPU. To do so, use the following command:

```
no ppp multilink fragmentation
```

Preventing Process Takeover

On occasion certain processes can be so demanding that they prevent other processes from using the CPU. The default maximum time for a single process to execute is 200 ms. However, it can be beneficial to set a limit that allows the vast majority of processes to execute while preventing long processes from dominating. To prevent exceptionally busy processes from starving others for CPU processing power, Cisco recommends the following:

```
process-max-time 30
```

Scaling AAA Processing

Use multithreaded AAA processing to provide for a load-sharing distribution of processes. This is illustrated in Other AAA Options, page 2-27. Note the caution there, and adjust the number of processes with care.

To see, for example, the processes that are related to PPP authorization, use the following command:

```
show processes cpu | include PPP auth
```

Optimizing Access Lists

To minimize unnecessary processing burdens resulting from the use of access control lists (ACLs), Cisco recommends the following general guidelines.

- Use the smallest number of lists possible to accomplish your objectives. You may need to rethink the design of your lists from time to time in order to make them as efficient as possible.
- Where possible, apply ACLs on a per-user basis.
- Where possible, apply ACLs on incoming interfaces. This minimizes unnecessary packet processing on the receiving platform.
- Define **allows** as close to the top of the list as possible.
- Define **deny all** at the end of the list. This makes it possible to monitor how hard the access list is working, whereas an *implicit deny* at the end of the list does not.

Platform-Specific Considerations

There are a variety of issues related to the use of Cisco Express Forwarding (CEF) and cache that need to be considered.

CEF optimizes network performance and scalability for networks with large and dynamic traffic patterns. It is less CPU-intensive than fast switching route caching. Distributed CEF, or dCEF, is a default on some platforms.

To enable CEF, use the **ip cef** command in global configuration mode. To disable CEF, use the **no** form of this command. The keyword **distributed** enables dCEF.

There are also cache settings (related to cache aging and I/O caching) that can help improve performance. Table 2-1 lists recommended CEF and cache settings for a variety of Cisco access platforms used in the Cisco ASAP Solution.

Table 2-1 Cisco Access Platforms and Recommended CEF and Cache Settings

Cisco Platform	CEF Recommendation	Cache Recommendation	Notes
Cisco AS5300	Disable	**ip cache-ager 20 3 3**	Speed up cache aging (see Caution below)
Cisco AS5350, Cisco AS5400	Pre-12.2(2)XB: Disable	**io-cache enable**	Ensure I/O cache is enabled
		ip cache-ager 20 3 3	Speed up cache aging
	Post-12.2(2)XB: Enable	**no io-cache enable**	Do NOT enable I/O caching
Cisco AS5800	Enable	—	—
Cisco AS5850	Enable	—	AS5850 uses dCEF, which is on by default. Disabling CEF has a major negative impact on the CPU

Caution Do not enable cache aging if you are using multilink PPP or VPDN.

Optimizing Modems

Recommendations for modem management include the following topics:

- Managing Modem Recovery
- Defining Basic Modem Capability
- Suppressing Modem Startup Tests and Autotests

Managing Modem Recovery

Modems may occasionally stop working. However, reloading the firmware generally resets the modem. The gateway can identify which DSPs have gone out of operation, and automatically reloads their firmware with minimal impact on end users or gateway capacity. Do the following for basic modem management.

Step 1 Use the following command to see the active statistics of all SPEs (service processing engines), a specified SPE, or a specified SPE range serving modem (and voice) traffic.

```
show spe modem active
```

This is used in the same way the **show modem** command is used for MICA modems. (The **show modem** command is not supported on the Cisco AS5350 or Cisco AS5400.)

Note The term SPE refers to the universal port card. For details refer to Managing and Troubleshooting the Universal Port Card at the following URL:
http://www.cisco.com/univercd/cc/td/doc/product/access/acs_serv/as5350/sw_conf/53swcg/54nextpt.htm

Caution Modem commands differ between MICA and NextPort modems. The syntax for the latter is that used for universal gateways. Refer to Comparing NextPort SPE Commands to MICA Modem Commands at the following URL:
http://www.cisco.com/warp/public/76/nextport_compare.html

Step 2 Use the **spe** command set, as in the following example, to configure recovery thresholds and download parameters.

```
spe recovery port-threshold 8
spe recovery port-action recover
spe download maintenance time 2:00
spe download maintenance max-spes 8
spe download maintenance window 90
```

Note Refer to Chapter 3, “Basic Configuration Using the Command-Line Interface,” of *Cisco AS5350 and Cisco AS5400 Universal Gateway Software Configuration Guide*, at the URL at the following URL:
http://www.cisco.com/univercd/cc/td/doc/product/access/acs_serv/as5350/sw_conf/53swcg/

Tip For more details of setting failure thresholds and configuring download times, refer to Configuring Modem Recovery at the following URL:
http://www.cisco.com/warp/public/76/modem-recovery.html

Defining Basic Modem Capability

For modems attached to asynchronous lines, a predefined modem capability, or *modemcap*, is used as an initialization script. That script facilitates the proper operation of the Cisco modem software in handshaking with and responding to calls from the user’s dial-in modem. The Cisco IOS maintains a set of built-in modemcaps for various internal and external user modems. A variable command option, *modemcap_name*, is used to represent a variety of modem types made by a variety of manufacturers.

Note For more detail refer to Modem-Router Connection Guide at the following URL:
http://www.cisco.com/warp/public/76/9.html

Do the following to create a minimum modemcap that will improve handshaking efficiency.

Step 1 Use the generic syntax to define a new modemcap.

```
modem autoconfigure type <type>
```

where *type* in this case is not an existing modem type, but rather, for example, *MyGenericModemcap* (an arbitrary name).

Step 2 Now use the following global configuration command **modemcap edit** to edit the new modemcap. The syntax is as follows:

```
modemcap edit modemcap_name miscellaneous <initialization_string>
```

So, for our example we have

```
modemcap edit MyGenericModemcap &F
```

Note ***&F*** represents the built-in MICA and NextPort modems, and may be used with many modems to reset them to their factory defaults.

Caution Do not use a preceding **AT** or terminating **&W**. Also, for this method to work, the modem must be configured with **echo** and **response** codes turned on. These are common factory defaults, but if they are not, a reverse telnet command to the modem will be required to turn them on.

Suppressing Modem Startup Tests and Autotests

Caution Make sure that startup tests and autotests are *never* enabled. Such tests, unless required, will have a negative impact on network operations.

The following is the command syntax for suppressing startup tests or autotests on universal gateways, which use SPEs:

```
no port modem startup-test | autotest
```

Use two separate lines to turn off both test types.

Optimizing SNMP

Cisco recommends that you disable traps on serial D-channel interfaces, but allow them to be enabled if a D-channel does go down.

Step 1 Disable traps on serial D-channel interfaces.

```
no snmp trap link-status
```

Step 2 Enable traps if a D-channel goes down. This is a global command.

```
snmp-server enable traps isdn layer2
```

Caution Generally speaking, because of the messaging interactions required, be selective when you enable SNMP features and options.

Using Virtual Access Interfaces to Optimize Dynamic Interface Configuration

Virtual access interfaces are logical entities—configurations for a serial interface that are not tied to a physical interface. One way to create virtual access interfaces is to use *virtual template* interfaces. In this case, the interfaces are *cloned* dynamically from a predefined configuration template for dial-in services. For example, when a user dials in, a predefined configuration template is used to configure a virtual access interface. When the user is done, the virtual access interface goes down and the resources are free for other dial-in uses.

Each virtual access interface can clone from only one template. However, some applications can take configuration information from multiple sources :*virtual profiles* can take configuration information from (a) a virtual template interface, (b) interface-specific configuration information from a user stored on an AAA server, (c) network protocol configuration from a user stored on an AAA server, or (d) all three. A virtual profile is a unique Point-to-Point Protocol (PPP) application that can create and configure a virtual access interface dynamically when a dial-in call is received, and tear down the interface dynamically when the call ends. The use of both templates and AAA configuration sources results in a unique virtual access interface for each dial-in user.

In addition, a *precloning* feature causes virtual access interfaces to be cloned in advance on the gateway, reducing the load on the system during call setup.

In summary, a significant feature of virtual profiles, virtual templates, and precloning is that these features reduce the demands on the gateway CPU. Choose one or both of the following options, as needed:

- Creating Virtual Access Interfaces Selectively
- Precloning Virtual Access Interfaces

Creating Virtual Access Interfaces Selectively

Do the following to create virtual access interfaces on the inbound connection as required.

Note For further information, refer to Configuring Virtual Template Interfaces at the following URL: http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fdial_c/fnsprt8/dafvrtmp.htm

Step 1 In global configuration mode, create a virtual template interface and enter interface configuration mode.

```
interface virtual-template <number>
```

Step 2 Enable IP without assigning a specific IP address.

```
ip unnumbered ethernet 0
```

Step 3 Enable PPP encapsulation on the virtual template interface.

```
encapsulation ppp
```

Step 4 Create virtual-access interfaces only if the inbound connection requires one.

```
virtual-profile if-needed
```

Precloning Virtual Access Interfaces

Do the following to specify the number of virtual-access interfaces to be created and cloned from a specific virtual template.

Note For further information, refer to PPP Autosense at the following URL:
http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121limit/121dc/121dc1/auto_ppp.htm

In global configuration mode, preclone virtual access interfaces as follows:

```
virtual-template <template-number> pre-clone <number>
```

In other words, specify the number of virtual-access interfaces (*number*) to be created and cloned from a specific virtual template (*template-number*).

Additional General Recommendations

There are a variety of Cisco IOS-based configuration settings that can also improve performance. If you have not already implemented the following, Cisco recommends that you review these topics and implement the respective commands.

Delay Trunk Activation

You can enable trunks to be activated when a defined percentage of SPEs (system processing engines) are ready to process calls, with the following command.

```
trunk activate port-threshold percent
```

This prevents the platform from attempting to accept calls before a sufficient number of SPEs are ready.

Note Refer also to Setting the Port Threshold for the Trunk Card at the following URL:
http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t5/dt_port.htm

Enable Passive Header Compression

Passive TCP header compression can help improve efficiency.

```
ip tcp header-compression passive
```

Note On SLIP (Serial Line Internet Protocol) lines, the **passive** option prevents transmission of compressed packets until a compressed packet arrives from the asynchronous link, unless a user specifies SLIP on the command line. For PPP, this option functions the same as the **on** option.

Optimize Line Configuration for Dial Service

Where dial-in only service is to be supported, the following commands will optimize the handling of calls:

```
modem Dialin
transport input none
```

Special Topics

The following special topics are presented in this section:

- Enabling Modem Features: V.44 and V.92
- Managing Echo Cancellation
- UG and GK Configuration Requirements for Microsoft NetMeeting with T.38 Fax Relay

Enabling Modem Features: V.44 and V.92

This section provides resources for enabling V.44 and V.92 features that are available in Cisco AS5350 and Cisco AS5400 universal gateway modem firmware. (These features are also available on Cisco AS5300 modems.)

V.44 Features

ITU-T standard V.44 is a compression algorithm known as LZJH (for Lempel-Ziv-Jeff-Heath). V.44 LZJH compression increases upload and download speeds, making Internet access and Web browsing faster, and also improving the call success rate.

For more information on this feature, as well as how to implement it, refer to the feature module V.44 LZJH Compression for Cisco AS5350 and Cisco AS5400 Universal Gateways at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122limit/122x/122xb/122xb_2/ft_v44.htm

V.92 Features

A new ITU-T modem standard, V.92, has been developed to enhance the existing V.90 standard. V.92 provides faster upstream speeds in analog (client) to digital (ISP) modem connections, while making possible such features as quicker modem negotiation and a modem-on-hold (MOH) capability. These new capabilities are addressed, respectively, by the following feature enhancements to the Cisco IOS and the feature card firmware:

- Quick Connect
- Modem on Hold

Related statistics are also collected by the feature card, for storage in the Cisco IOS software.

Quick Connect

Quick connect (QC) provides a standard method of reducing the negotiation time by storing analog channel characteristics (such as equalizer taps and echo canceller taps) in nonvolatile memory on the modem feature card. Similarly, digital characteristics are also stored. After characteristics have been established and stored, on subsequent calls to a server modem equipped to train fast, the client modem examines the answer tone to verify that line conditions match the saved parameters. If they match, an fast connection is attempted. (Negotiation times can be reduced from 20 to 10 seconds.) If they do not, a regular V.90 handshake commences.

For more information on this feature, as well as how to implement it, refer to the feature module V.92 Quick Connect for Cisco AS5350 and Cisco AS5400 Universal Gateways at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122limit/122x/122xb/122xb_2/ftv92qc.htm

Modem on Hold

Modem on hold (MOH) was designed to resolve a problem that resulted in a large number of trouble calls to the ISP. Often users with a single line do not disable call waiting when they are online, and a call waiting signal looks to a modem like a line disconnect. Depending on how the modem is configured, this can often result in the modem hanging up. While some users may prefer this behavior, a hung-up modem is an inconvenience to other users.

Note The V.92 MOH feature is designed for use on lines that are configured for call waiting. A call waiting (incoming) voice call signals the suspension of the modem session. If call waiting is not enabled, other callers simply receive a busy signal, and the modem session is not interrupted. MOH can also be controlled on a per-call basis by means of a RADIUS server.

MOH allows a dial-in user with a single line to suspend a modem session to answer an incoming voice call—or place an outgoing call while engaged in a modem session. After the session is suspended, the ISP modem listens to the original connection and waits for the user’s modem to resume the connection. The interval during which the server remains alert to the reconnection is called the “call-waiting survival,” and is configurable.

Caution Call-waiting tones vary widely from country to country. Configuring the MOH feature in a specific country for which the client modem does not recognize the tones can cause the modem to disconnect.

For more information on this feature, as well as how to implement it, refer to the feature module V.92 Modem on Hold for the Cisco AS5350 and Cisco AS5400 Universal Gateways at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122limit/122x/122xb/122xb_2/ftv92moh.htm

Managing Echo Cancellation

Overview

In Cisco AS5400 and AS5350 UGs, echo cancellation is enabled by default, with tail-delay coverage set at 8 milliseconds. However, if you are using the Cisco echo canceller in the UGs, it is important to determine the maximum echo-path tail delay and IP network delay that may exist in your network. In addition, other services (such as wireless) may add additional echo-path delays. If echo delay is longer than the provisioned tail length, echo cancellation will not work.

In general, you should enable echo cancellation in networks where predicted echo-path delays exceed 32 milliseconds. Also, if you plan to use external echo cancellation, Cisco recommends that you disable the echo cancellers in the UGs. This will save memory and other platform resources.

Note Information about echo cancellation terminology and guidelines for network design can be found in ITU recommendation G.168, available at http://www.itu.org. See also Echo Analysis for Voice over IP at the following URL:
http://www.cisco.com/univercd/cc/td/doc/cisintwk/intsolns/voipsol/ea_isd.htm

The following example echo-cancellation configurations are presented:

- Disabling Echo Cancellation
- Changing Tail-Delay Coverage
- Typical Echo-Cancellation Settings

Disabling Echo Cancellation

The following commands illustrate how to disable echo cancellation on a voice port.

Caution Because voice ports are created automatically when an ISDN D-channel or CAS signaling is assigned to a controller, you must determine which voice ports require echo cancellation and which do not. In this SS7 example there is only one voice port, as SS7 requires the instantiation of only one voice port (1/0:1:D), to support the serial D-channel.

```
5400#conf t
5400(config-voiceport)#voice-port 1/0:1:D
5400(config-voiceport)#no echo-cancel enable
5400(config-voiceport)#
```

Changing Tail-Delay Coverage

If you decide to use echo cancellation in your UGs, you may have different needs regarding the tail-delay coverage setting. The following commands illustrate how to change the tail-delay coverage setting.

```
5400#conf t
5400(config)#voice-port 1/0:1:D
5400(config-voiceport)#echo-cancel coverage
5400(config-voiceport)#echo-cancel coverage ?
  128  128 milliseconds echo canceller coverage
  16   16 milliseconds echo canceller coverage
  24   24 milliseconds echo canceller coverage
  32   32 milliseconds echo canceller coverage
  64   64 milliseconds echo canceller coverage
  8    8 milliseconds echo canceller coverage

5400(config-voiceport)#echo-cancel coverage 128 <---see Note below
5400(config-voiceport)#exit
```

Note This sets the echo canceller to cover a tail delay of 128 milliseconds.

Typical Echo-Cancellation Settings

Here are some typical echo-cancellation settings, most of which are defaults. In this SS7 case, the settings are mapped from this port to a port related to a path in the echo canceller.

```
5400#sho voice port

ISDN 1/0:1:D - 1/0:1:D <--serial D-channel for SS7 RLM group (T1 controllers 1/0:1-1/0:14)
 Type of VoicePort is ISDN
 Operation State is DORMANT
 Administrative State is UP
 No Interface Down Failure
 Description is not set
 Noise Regeneration is enabled
 Non Linear Processing is enabled
 Non Linear Mute is disabled
 Non Linear Threshold is -21 dB
 Music On Hold Threshold is Set to -38 dBm
 In Gain is Set to 0 dB
 Out Attenuation is Set to 0 dB
 Echo Cancellation is enabled
 Echo Cancellation NLP mute is disabled
 Echo Cancellation NLP threshold is -21 dB
 Echo Cancel Coverage is set to 128 ms
 Playout-delay Mode is set to default
 Playout-delay Nominal is set to 60 ms
 Playout-delay Maximum is set to 200 ms
 Playout-delay Minimum mode is set to default, value 40 ms
 Playout-delay Fax is set to 300 ms
 Connection Mode is normal
 Connection Number is not set
 Initial Time Out is set to 10 s
 Interdigit Time Out is set to 10 s
 Call Disconnect Time Out is set to 60 s
 Ringing Time Out is set to 180 s
 Wait Release Time Out is set to 30 s
 Companding Type is u-law
 Region Tone is set for US
 Station name None, Station number None
```

UG and GK Configuration Requirements for Microsoft NetMeeting with T.38 Fax Relay

Applications that are not compliant with T.38 Fax Relay, such as Microsoft NetMeeting, may not work properly unless certain configurations are applied to the dial peer as well as to the gatekeeper. Adjustments need to be made to the NetMeeting application, the UG, and the GK, as discussed below. There are three basic components to configuring Microsoft NetMeeting with T.38 Fax Relay:

- Configuring the NetMeeting Application
- Configuring the UG for NetMeeting
- Configuring the GK for NetMeeting

Configuring the NetMeeting Application

Step 1 Choose **Tools** > **Options** > **Advanced Calling**.

Step 2 Select Use a Gatekeeper to Place Calls.

This will allow you to enter a phone number in the Call menu.

Configuring the UG for NetMeeting

On the gateway, if you are using the global command to configure T.38 Fax Relay service (see Enabling T.38 Fax Relay Service, page 2-21), rather than configuring individual dial peers, you must do the following on the incoming VoIP dial peer that serves PC-to-phone calls.

Step 1 Enter the command **fax rate disable**.

Step 2 Enter the command **codec G711ulaw**.

If these are not configured, calls will have only a one-way audio path. Note the following.

```
dial-peer voice 1000 voip
 description Incoming PC Calls
 incoming called-number 9011081...
fax rate disable <---must be configured
codec G711ulaw <---must be configured
no vad
```

In addition, NetMeeting currently causes a digital data bearer capability to be built into the outgoing SETUP message on egress PC-to-phone speech calls from the Cisco gateway. Below is an example of what can be done to remedy this.

Step 3 Configure **bearer-cap** to 3100 Hz, as shown.

```
voice-port 2/0:D
echo-cancel coverage 64
bearer-cap 3100Hz <---must be configured
```

Configuring the GK for NetMeeting

Gatekeeper provisioning is discussed in greater detail in Chapter 3, "Configuring Optional Network Components." However, for convenience, the following information is presented here.

In order for the gatekeeper to allow calls from a NetMeeting PC, you must configure a series of **no use-proxy** statements. Configure **no-use-proxy** as in the following example (zone GK names will vary):

```
no use-proxy z3-gk1 remote-zone z1-gk1 inbound-to terminal
no use-proxy z3-gk1 remote-zone z1-gk1 outbound-from terminal
no use-proxy z3-gk1 default inbound-to terminal
no use-proxy z3-gk1 default outbound-from terminal
```

CHAPTER 3

Configuring Optional Network Components

Introduction

This chapter discusses key provisioning issues related to network components other than the gateway (covered in Chapter 2, "Configuring a Universal Gateway for Service"), and that are not commonly considered network management applications (covered in Chapter 4, "Using Management and Shared Support Services").

⚠ **Caution** Certain features vary from one Cisco IOS release to another, as do configuration requirements. Before configuring a platform, always refer to the latest release notes for the solution. The release notes for the Cisco ASAP Solution are available at the following URL:
http://www.cisco.com/univercd/cc/td/doc/product/access/solution/asap/index.htm

Establishing Additional Components to Support Dial

Dial access networks, as they must originate at the edge of the PSTN, must commonly (although not always) support SS7 signaling. Where SS7 signaling is required, the Cisco ASAP Solution relies on the Cisco SS7 Interconnect for Access Gateways Solution, which uses a Cisco SC2200 node. (A Cisco SC2200 node is also used to support SS7 signaling for voice services.)

For details, refer to Cisco SS7 Interconnect for Access Servers Solution Release 2.2 at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/access/sc/rel7/soln/das22/index.htm

Note There are special issues that must be taken into account when Cisco RPMS is used with SS7 signaling. Refer to SS7 Resource Groups, page 4-31.

Establishing Additional Components to Support Voice

VoIP networks rely upon the H.323 standard for the transmission of real-time audio, video, and data communications over packet-based networks. Key components of an H.323-based network are the gateways (GWs), gatekeepers (GKs), and directory gatekeepers (DGKs) that signal among themselves using the H.323 RAS (Registration, Admission, and Status Protocol), in order to establish communications paths before bearer traffic is transmitted. Support for SS7 signaling may or may not be required.

Note In the case of the Cisco ASAP Solution, which supports both voice and dial services on a single platform, the term universal gateway, or UG, is used where GW would otherwise be used.

Provisioning SS7 Interconnect for Voice

Where SS7 must be supported, the Cisco ASAP Solution relies on the Cisco SS7 Interconnect for Voice Gateways Solution. Refer to Cisco SS7 Interconnect for Voice Gateways Solution, Release 1.3 at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/access/sc/rel7/soln/voip13/index.htm

For an overview of the architecture of the Cisco SC2200 node and its components (including the Cisco 2611 SLT), as well as concise configuring and installation information, refer to Chapter 5, “Provisioning SS7-Based POPs,” in the *Cisco Wholesale Voice Solution Design and Implementation Guide*, at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/access/sc/rel7/soln/wv_rel1/wvpg/index.htm

Designing and Provisioning H.323 VoIP Networks

The fundamentals of designing and provisioning H.323 networks for VoIP services are well covered in the *Cisco Wholesale Voice Solution Design and Implementation Guide*, at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/access/sc/rel7/soln/wv_rel1/wvpg/index.htm

Chapter 2, “Provisioning the Gatekeeper Core,” discusses the gatekeeper core and its components, as well as dial plans and traffic management. The following topics are covered there:

- Dial Plans and Number Normalization

  (Also see Chapter 4, “Designing a Solution,” in the *Cisco ASAP Solution Overview and Planning Guide* at the following URL:
  http://www.cisco.com/univercd/cc/td/doc/product/access/solution/asap/overview/index.htm)
- Understanding Configuration Basics
- Establishing Core Components

Note Within the context of the Cisco ASAP Solution, Cisco AS5300 gateways support dial services only.

Caution Not all CAC features will be available in early releases of the Cisco ASAP Solution.

Establishing a Gatekeeper

Configuring the gatekeeper is straightforward.

Caution Applications that are not compliant with T.38 Fax Relay, such as Microsoft NetMeeting, may not work properly unless certain configurations are applied to the dial peer as well as to the gatekeeper. For details, see UG and GK Configuration Requirements for Microsoft NetMeeting with T.38 Fax Relay, page 2-50.

Note Refer to Configuring the Gatekeeper, in Chapter 2, “Provisioning the Gatekeeper Core,” of the *Cisco Wholesale Voice Solution Design and Implementation Guide* at the following URL: http://www.cisco.com/univercd/cc/td/doc/product/access/sc/rel7/soln/wv_rel1/wvpg/index.htm

Step 1 Confirm that a time zone is configured.

```
clock timezone edt -4
ip subnet-zero
```

Step 2 Enable the Cisco VoIP CAC with RSVP feature. See Call Admission Control and RSVP, page 4-2.

```
call rsvp-sync
!
interface FastEthernet0/0
 ip address 10.41.7.50 255.255.0.0
 duplex full
!
interface FastEthernet1/0
 ip address 10.40.7.50 255.255.0.0
 no ip mroute-cache
 duplex full
 ntp broadcast client
!
ip default-gateway 10.100.10.10
ip classless
ip route 0.0.0.0 0.0.0.0 10.40.0.1
no ip http server
```

Step 3 Establish a gatekeeper identity, as well as zones, gateway priorities, and a technology prefix.

```
gatekeeper
 zone local z1-gk1 ASAP_voice 10.40.7.50
 zone remote z2-gk1 ASAP_voice 10.70.7.50 1719
 zone remote z3-gk1 ASAP_voice 10.80.7.50 1719
 zone prefix z1-gk1 901103* gw-priority 10 z1-gw1
 zone prefix z1-gk1 901103* gw-priority 0 z1-gw2 z1-gw3
 zone prefix z1-gk1 901108* gw-priority 10 z1-gw2
 zone prefix z1-gk1 901108* gw-priority 0 z1-gw1 z1-gw3
 zone prefix z1-gk1 901110* gw-priority 10 z1-gw3
 zone prefix z1-gk1 901110* gw-priority 0 z1-gw1 z1-gw2
 zone prefix z2-gk1 902*
 zone prefix z3-gk1 903*
 gw-type-prefix 1#* default-technology
 no shutdown
```

Establishing a Directory Gatekeeper

Depending on the size of the network to be managed, directory gatekeepers and alternate directory gatekeepers may also be required. Configuration examples are presented in Chapter 2, “Provisioning the Gatekeeper Core,” of the *Cisco Wholesale Voice Solution Design and Implementation Guide* at the following URL:
http://www.cisco.com/univercd/cc/td/doc/product/access/sc/rel7/soln/wv_rel1/wvpg/index.htm

Additional Server Support for Dial and Voice

As noted in Chapter 2, “Configuring a Universal Gateway for Service,” a Cisco RPMS or Cisco AR may be required for accounting and management purposes. See the following sections, respectively:

- Enabling Cisco RPMS 1.x, page 4-23
- Enabling Cisco AR, page 4-32

CHAPTER 4

Using Management and Shared Support Services

Introduction

This chapter presents key issues related to the management and design of a Cisco ASAP Solution, including links to detailed installation and provisioning information for the following tools:

- Resource and Network Management

  Discusses how to ensure quality of service (QoS) in mixed voice and data networks, and other traffic-related design issues. Includes bothCisco IOS-based services such as basic and enhanced call admission control (CAC), as well as application-based resource and element management applications.

- Additional QoS Remedies

  Includes IP precedence and low latency queuing (LLQ).

- Traffic Engineering Guidelines

  Architecture- and bandwidth-related tips for eliminating traffic bottlenecks, including both edge and core issues.

- L2TP Tunneling and VPDNs

  The details of enabling Layer 2 Tunnel Protocol virtual private dial networks on both the universal gateway (UG) and the tunnel server.

- Enabling Cisco RPMS 1.x

  The details of enabling Cisco RPMS on a UG, including issues related to SS7 interconnect.

- Enabling Cisco AR

  An overview of the functions provided by the Cisco Access Registrar (AR), a RADIUS-based AAA server, with references to user documentation and an installation guide.

- Using Cisco RLM

  An overview of the features of Cisco Redundant Link Manager (RLM), with references.

- Configuring Multilink PPP

  An overview of multilink PPP (MLP) and multichassis multilink PPP (MMP), with references.

- Enabling SNMP

  An overview of the features of Simple Network Management Protocol (SNMP), with references.

- Using MIBs

A link to management information base files and application notes, with a list of MIBs suitable to the Cisco ASAP Solution.

Resource and Network Management

There are three basic steps to implementing satisfactory QoS:

- *Classification*: Mark the packet to indicate its type of service.
- *Scheduling*: Assign packets to one of multiple queues (based on the above classification) to expedite (in the case of VoIP) the delivery of packets through the network.
- *Provisioning*: Calculate the required bandwidth for all applications, including element overhead.

Note For more information about the above and other issues, refer to Quality of Service for Voice over IP at the following URL:
http://www.cisco.com/univercd/cc/td/doc/cisintwk/intsolns/qossol/qosvoip.htm

To help ensure QoS, a variety of resources can be managed from the Cisco IOS CLI by means of the following features:

- Call Admission Control and RSVP
- Low-Latency Queuing
- RSVP/LLQ Integration

These features are discussed below.

Call Admission Control and RSVP

This section presents the details of CAC features, both basic and enhanced. The latter includes Resource Reservation Protocol (RSVP).

Note For an overview of contention types and remedies, as well as both basic and enhanced CAC, refer to Contention in Chapter 4, “Designing a Solution,” in the *Cisco ASAP Solution Overview and Planning Guide* at the following URL:
http://www.cisco.com/univercd/cc/td/doc/product/access/solution/asap/index.htm

RSVP is an IETF standard designed to support resource (such as bandwidth) reservations through networks of varying topologies and media. QoS requests are propagated to all routers along the data path, allowing the network to reconfigure itself to meet the desired level of service. RSVP is a remedy for voice/voice contention—the impact on all voice calls in a link caused by link overutilization—by ensuring the end-to-end availability of bandwidth. Once a voice link is utilized between 80 and 100 percent of capacity, jitter becomes significant. Jitter (the phase shift of digital pulses) results in the latency of voice packets, and an undesirable listening experience. Once link utilization exceeds 100%percent (statistically), the entire link is lost. RSVP is required if any link in the access network can become congested with voice traffic. It is implemented on the UG, as well as on any node (such as an edge router) in the access network.

RSVP is an enhancement to CAC that ensures QoS in Cisco H.323 VoIP networks. Its principles are identical to those of the IETF standard. RSVP-based CAC allows applications to request end-to-end QoS guarantees from the network. The Cisco VoIP Call Admission Control using RSVP feature synchronizes

RSVP signaling with H.323 Version 2 signaling to ensure that the bandwidth reservation is established in both directions before a call moves to the alerting phase (ringing). This ensures that the called party's phone rings only after the resources for the call have been reserved. Using RSVP-based CAC, VoIP applications can reserve network bandwidth and react appropriately if bandwidth reservation fails.

Note For more information, refer to following documents at their respective URLs:

VoIP Call Admission Control:
http://www.cisco.com/univercd/cc/td/doc/cisintwk/intsolns/voipsol/cac.htm

VoIP Call Admission Control Using RSVP:
http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t5/dt4trsvp.htm

Call Admission Control for H.323 VoIP Gateways:
http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122limit/122x/122xa/122xa_2/ft_pfavb.htm

Like IETF RSVP, RSVP-based CAC is required if any link in the access network can become congested with voice traffic. It is implemented on the UG, as well as on any node (such as an edge router) in the access network.

Table 4-1 lists the call-denial rejection criteria (monitored resources or parameters) for voice and data calls.

Table 4-1 Call Types and Rejection Criteria

Contention Type	Rejection Criteria (Monitored Resource or Parameter)
Incoming dial	CPU utilization
	Memory utilization
Incoming voice	CPU utilization
	Memory utilization
	Call arrival rate
	RSVP
	Voice quality
	Round-trip delay in VoIP network
Outgoing voice	CPU utilization
	Memory utilization

Basic Call Admission Control

The key to managing contention is managing gateway resources. This differs between the PSTN side and the Cisco ASAP network side.

On the PSTN side, calls are neither delivered nor accepted if any set of required resources are all in use. In this case the following resources are monitored:

- The number of DS0s that are currently accommodated
- The number of DSPs that are currently in use

- The load on the HDLC framers

The above parameters are monitored by default on both ingress and egress UGs. If either of the above parameters are at a maximum at either end of the network, the call is not set up.

Enhanced CAC Features

The following discussion introduces the enhanced CAC commands that work within the H.323 protocol suite.

Resource Availability Indicator

On the Cisco ASAP network side, the gateway informs the GK if a resource threshold is exceeded. The flag is the RAI, or Resource Availability Indicator. The RAI is an H.323 CAC feature that informs the GK when no circuits (DS0s) are available.

The GK selects the UG on the basis of the UG's RAI status. In this case the following resources are monitored:

- The number of DS0s that are currently accommodated
- The number of DSPs that are currently in use

RAI messages indicate both the availability and unavailability of a UG, depending on the threshold for each that the user can set. RAIs let the GK select the best available UG at the outset, increasing call-completion rates and lowering postdial delay. After the GK receives an RAI from an overburdened UG, it will not assign calls to that UG.

There are two load thresholds: A high value determines when the UG sends the GK an "unavailable" RAI, and the low value determines when the UG sends the GK an "available" RAI. The syntax (available under **config-gateway**) is as follows:

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

Note In initial releases of the Cisco ASAP Solution, CPU and memory utilization are not yet included in the RAI message.

Note For examples of RAI and CAC, see Using Traffic Management Features in Chapter 2, "Provisioning the Gatekeeper Core," of the *Cisco Wholesale Voice Solution Design and Implementation Guide* at the following URL:
http://www.cisco.com/univercd/cc/td/doc/product/access/sc/rel7/soln/wv_rel1/wvpg/index.htm

Refer also to VoIP Call Admission Control, at the following URL:
http://www.cisco.com/univercd/cc/td/doc/cisintwk/intsolns/voipsol/cac.htm

That document also discusses RAI and PSTN fallback.

Further information about the PSTN fallback feature is also available at the following URL:
http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t3/dtpstnfb.htm

Note The discussion below presents only a generalized syntax and basic parameters. For the details of provisioning, including examples and related commands, refer to Call Admission Control for H.323 VoIP Gateways, at the following URL:
http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122limit/122x/122xa/122xa_2/ft_pfavb.htm

A variety of features have been added to CAC to monitor both UG and network resources. On the UG side, the user can now define thresholds for monitoring UG health, as well as the actions that will take place when a threshold is exceeded.

If system (gateway) resources are not available to admit the call, two kinds of actions are possible:

- System denial: busies out an entire T1 or E1
- Per-call denial: disconnects or hairpins the call (back to the PSTN), or plays a message or tone

If the interface-based resource is not available to admit the call, the call is dropped from the session protocol (in this case H.323).

There are options for call treatment, and restrictions can be placed on call rates. On the network side, both end-to-end bandwidth and end-to-end voice quality can be monitored. These enhancements are discussed below.

Gateway Health Resources

PSTN access gateways (UGs) can be monitored for overall health with respect to a variety of parameters:

- Average and 5-second CPU load
- Aggregate number of voice calls
- Processor and I/O memory utilization

Note The Cisco IOS features and commands discussed below are available with Cisco IOS Release 12.2(2)XA and later.

The global configuration command is **call threshold**, with the basic syntax as follows:

```
call threshold global <trigger-name> low <percent> high <percent> <busyout | treatment>
```

With a global resource trigger such as the above, the default is **busyout** plus **treatment**. These global-only options work as follows.

With the option **busyout**, the Cisco Resource Unavailable Signaling feature set uses an *autobusyout* feature to transmit a busy signal on all T1/E1 channels in a trunk if the resource is not available. This feature works for both CAS and PRI trunks.

- With a CAS busyout, a “local resources are unavailable” message is sent.
- With a PRI busyout, either service messages are sent, or a disconnect occurs with an ISDN cause code that signals “resources are unavailable.”

Table 4-2 lists the options for the triggers (*trigger-name*).

Table 4-2 Call Threshold Trigger Options

trigger-name	Description
cpu-5sec	CPU utilization in the last 5 seconds
cpu-avg	Average CPU utilization
io-mem	I/O memory utilization
proc-mem	Processor memory utilization
total-calls	Total number of calls
total-mem	Total memory utilization

Values for **low** and **high** range from 1 to 100 (percent) for utilization triggers and from 1 to 10,000 (calls).

Note The **call threshold** command can also be applied to individual interfaces. However, generally only the **global** option will be of interest in a Cisco ASAP Solution network.

When thresholds are exceeded, the designer needs to know how to treat the rejected call. This is discussed in the following section.

Call Treatment

Call treatment following a threshold overrun can take various forms, depending on whether the resource-challenged gateway (UG) is an originating gateway (OGW) or terminating gateway (TGW). Requirements are different on the TGW because the network expects reasons for the call rejection. The options of the global configuration command **call treatment** determine how calls should be processed when local resources are unavailable. This indicates whether the call should be disconnected (with cause code) or hairpinned, or a message or busy tone should be played to the user.

The use of this command will vary, depending on whether it is used on the OGW or the TGW.

On the OGW

- Reject the call. The call is disconnected with a cause code.
- Play a message. ("We're sorry your call cannot be completed at this time. Please try again later.")
- TDM switches the call to the PSTN through a POTS dial peer. (This is known as hairpinning.)

The global configuration command is **call treatment**.

The basic syntax is as follows:

```
call treatment on
```

Caution This feature must first be turned *on*, as it is inactive by default.

```
call treatment action <reject | playmsg | hairpin>
```

The values of **action** are as follows:

- **hairpin**—The call is sent back to the PSTN.

- **playmsg**—Followed by the HTTP URL location of the audio file to be played, plays an audio file.
- **reject**—Disconnects the call and passes down a cause code.

On the TGW

- Define an ISDN reject code.
- Define a cause code.

The basic syntax in this case is as follows:

```
call treatment on
call treatment isdn-reject <cause-code 34-47>
call treatment cause-code <busy | no-qos | no-resource>
```

The parameters are as follows:

- **isdn-reject**—Selects the ISDN cause code.
- **cause-code**—Specifies to the caller the reason for the disconnect, with values as follows:
  - **busy**—The gateway is busy.
  - **no-qos**—The gateway cannot provide the quality of service level configured in the dial peer.
  - **no-resource**—The gateway has no resources available.

Call Rate Restriction

It is also possible to monitor the aggregate rate at which calls arrive, by using the global configuration command **call spike**. The syntax is as follows:

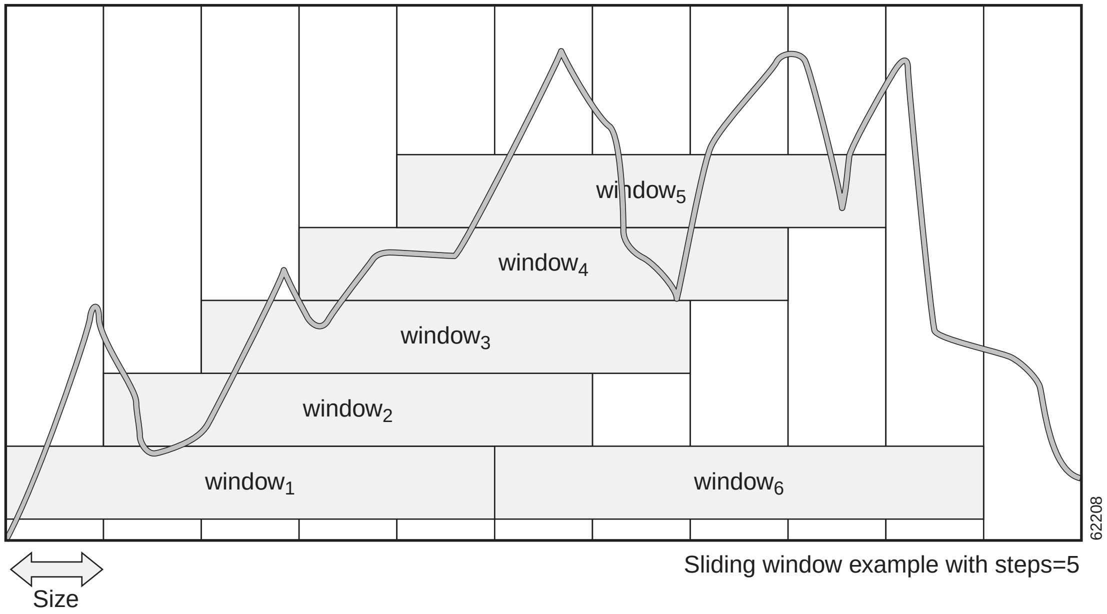
```
call spike <call-number> [ steps <number-of-steps> size <milliseconds> ]
```

The parameters are as follows:

- **call-number**—The number of incoming calls to set as the spike threshold. The range is from 1 to 2,147,483,647.
- **steps**—The number of steps in a sliding window. The range is from 3 to 10. (See discussion below.)
- **size**—The size of the step in milliseconds. The range is from 100 to 2000. (See discussion below.)

This configures the limit for the number of incoming calls (*call-number*) over the interval determined by *size*. Steps refer to the number of sliding windows that are applied to capture the numbers of incoming calls. This number is bursty, hence the term “spike.” Figure 4-1 illustrates the relationship between the *size* and *step* parameters in the sliding window approach. Each “size” interval forms the beginning boundary of a new window. As bursts increase and must be captured, the number of steps (and hence windows) will need to be increased.

Figure 4-1 Sliding Windows Applied to Monitor Number of Incoming Calls



End-to-End Bandwidth

It is important to ensure that bandwidth is reserved in both directions before the call moves to the alerting phase, so that the called party's phone rings only after all the resources for the call have been reserved. The CAC feature that does this in Cisco H.323v2 VoIP networks is enabled through Resource Reservation Protocol (RSVP), the IP service that allows applications to request end-to-end QoS guarantees from the network. (RAI and RSVP can be considered as being mutually exclusive.)

Note For more details, see VoIP Call Admission Control Using RSVP at the following URL:
http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t5/dt4trsvp.htm

The command (enabled by default) **call rsvp-sync** enables synchronization between RSVP and the H.323 voice signaling protocol.

First ensure that bandwidth is reserved in both directions before ringing occurs:

```
call rsvp-sync
```

To set a timer for reservation requests (limiting the number of seconds to wait before proceeding with call setup or releasing the call according to the configured QoS level in dial peers), the command option **resv-timer** is used, with the following syntax:

```
call rsvp-sync resv-timer <seconds>
```

The TGW knows what QoS is acceptable for the call, from its own configuration and the value included by the OGW in the H.323 SETUP message. If the TGW and the OGW are requesting a non-best-effort QoS and at least one reservation fails, the call will proceed as a best-effort call *only* if both gateways are willing to accept best-effort service. Otherwise, a Q.931 DISCONNECT message with cause code 49 (QoS unavailable) is generated.

End-to-End Voice Quality

It is important to ensure that delay, jitter, and packet loss between the ingress UG and remote IP addresses are within acceptable thresholds.

Voice quality can be determined by the degree of delay or packet loss, or can be based on ICPIF (the ITU G.113 Calculated Planning Impairment Factor). When a threshold is exceeded, the Cisco PSTN Fallback feature is invoked. Both ICPIF and PSTN fallback are discussed below.

Note For more information about ICPIF and PSTN fallback, refer to PSTN Fallback at the following URL: http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t3/dtpstnfb.htm

ICPIF Delay and Loss Thresholds

Delay and loss ICPIF thresholds use a feature called RTR (Response Time Reporter) to determine latency, delay, and jitter, in order to provide real-time ICPIF calculations before a call is established across an IP infrastructure. RTR packets emulate voice packets, receiving the same priority as voice throughout the entire network. RTR is superior to either data or ICMP ping packets for determining congestion levels.

Delay and loss thresholds are determined by the following **call fallback** command parameters:

```
call fallback threshold delay <delay-value> loss <loss-value>
```

The parameters are as follows:

- **delay**—Sets the delay value in milliseconds.
- **loss**—Sets the loss value in percent.

Alternatively, use the following to apply an ICPIF threshold to network traffic:

```
call fallback threshold icpif <threshold-value>
```

The parameter is as follows:

- **icpif**—Sets the ICPIF threshold value. The valid range is from 0 to 34.

Table 4-3 lists ICPIF threshold values and the corresponding speech quality they represent. When a threshold is exceeded, PSTN fallback is invoked. See PSTN Fallback, below.

Table 4-3 ICPIF Values

ICPIF Value	Speech Quality
5	Very good
10	Good
20	Adequate
30	Limiting case
45	Exceptional limiting case
55	Customers likely to react strongly

The general idea behind G.113 is to calculate an impairment factor for every piece of equipment along the voice path, then add all factors to obtain total impairment. There are different types of impairments (noise, delay, echo, and so on), and the ITU divides them into five categories.

Note For the latest revisions of ITU G.113, visit the International Telecommunication Union at http://www.itu.int.
You may also wish to consult with your Cisco account representative regarding the details of ICPIF provisioning.

PSTN Fallback

The Cisco PSTN Fallback feature has the following characteristics:

- Congestion in the IP network is monitored, and when congestion is found, calls are either (1) redirected to the PSTN, (2) redirected to an alternate IP destination, or (3) rejected.
- The user defines the congestion thresholds to meet the needs of the configured network.
- If the data network is congested at the time of call setup, calls are automatically routed to any alternate destination.
- Information about delay, jitter, and packet loss is provided for the configured IP addresses.
- A network traffic cache is used to maintain ICPIF and delay, loss, and jitter values that improve performance. Values are cached from a previous call, so that a new call does not have to wait for "probe" results before being admitted.

The network designer must then consider how to handle traffic when voice quality falls outside the defined thresholds. Here there are two options:

- Use alternative dial peers. The global configuration command **call fallback active** is required to determine whether calls should be accepted or rejected on the basis of a probe of network conditions, using alternative dial peers in case of network congestion.
- Monitor elements but do not implement fallback. The global configuration command **call fallback monitor** allows destinations to be monitored without fallback to alternate dial peers. There is no H.323 call checking or rejecting. To enable this, you must configure the following commands to set thresholds:
  - **call fallback threshold delay loss**
  - **call fallback threshold icpif**

  The above thresholds are ignored, but they enable the collection of statistics.

Caution PSTN fallback does ensure that a VoIP call is protected from the effects of congestion. That is the function of other QoS mechanisms such as IP Real-Time Transport Protocol (RTP) or low latency queuing (LLQ).

For details on using ICPIF within Cisco Voice Manager, refer to Managing Voice Quality with Cisco Voice Manager (CVM) and Telemate at the following URL:

http://www.cisco.com/warp/public/788/AVVID/cvmtelemate.html

Note Cisco CVM with Telemate provides limited provisioning support, and is not well-suited to large-scale service provider deployments. Applications from other vendors may work with CVM to provide more capability. CVM 2.0.2 is the only release currently supported.

Additional QoS Remedies

This section discusses the following additional remedies that can be applied to ensure QoS:

- IP Precedence
- Low-Latency Queuing
- RSVP/LLQ Integration
- Link Fragmentation and Interleaving

IP Precedence

IP precedence is a remedy for voice and data contention by marking traffic for different priority classes. This technique is required if any link in the entire network can become congested—an extremely likely possibility. IP precedence is implemented at the UG edge interfaces, both voice and modem.

Table 4-4 lists traffic classes and types, along with their IP precedence numbers.

Table 4-4 Traffic Classes and Types, with IP Precedence Numbers

Traffic Class	Traffic Type	IP Precedence Number
Voice bearer	RTP	5
Signaling	RTCP, RSVP, Q.931+/IP, H.323, etc.	3
Data	Best effort	0

Voice traffic is assigned the highest precedence, but related signaling is not far behind. Data, however, can tolerate latency with little effect on the user, and so is delivered simply in a “best effort” attempt.

Note For more information about IP precedence, refer to Quality of Service for Voice over IP at the following URL:
http://www.cisco.com/univercd/cc/td/doc/cisintwk/intsolns/qosvoip.htm

Low-Latency Queuing

The Cisco Low Latency Queuing (LLQ) feature, supported by the Cisco Resource Reservation Protocol (RSVP) feature, brings strict priority queuing to class-based weighted fair queuing (CBWFQ). Strict priority queuing allows delay-sensitive data such as voice to be dequeued and sent first (before packets in other queues are dequeued), giving delay-sensitive data preferential treatment over other traffic.

To guarantee the bandwidth required for voice, LLQ schedules signaling and voice traffic according to their traffic class. LLQ is implemented on any link in the network that can become congested by a combination of signaling, voice, and data traffic.

Note For more information about the Cisco Low Latency Queuing feature, refer to the following URL:
http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120t/120t7/pqcbwfq.htm

In addition, LLQ requirements vary according to link bandwidth. In high-speed (>1.5 Mbps) links, both signaling and voice traffic are placed in a priority queue, with data in a best effort queue. With low-speed (<1.5 Mbps) links, where there naturally is less bandwidth to be shared among all required traffic types, signaling is placed in a weighted queue, assigning sufficient bandwidth to guarantee against data drops. Voice traffic is placed in a priority queue, and data again in a best effort queue.

RSVP is a network-control protocol that provides a means for reserving network resources (primarily bandwidth), to guarantee that applications achieve the desired QoS across the network. LLQ is an efficient queuing implementation that improves upon the weighted fair queuing (WFQ) algorithm used by RSVP.

Note For additional information and examples, refer to RSVP Support for Low Latency Queuing at the following URL:
http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t3/rsvp_llq.htm

Refer also to Configuring RSVP Support for LLQ at the following URL:
http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fqos_c/fqcprt5/qcfrsllq.htm

RSVP/LLQ Integration

RSVP uses WFQ to provide fairness in flows and assign a low weight to a packet so it can attain priority. However, the RSVP queuing algorithm fails to minimize jitter. Whereas RSVP provides call admission control, the Cisco RSVP Support for Low Latency Queuing feature also provides the needed support for bandwidth and delay guarantees need for voice traffic.

Note For more information about the Cisco RSVP Support for Low Latency Queuing feature, refer to the following URL:
http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t3/rsvp_llq.htm

UGs have a software feature that sets and monitors CPU threshold to provide this service. This feature, known as the Cisco Call Admission Control Based on CPU Utilization feature, denies incoming calls that exceed a preconfigured threshold of system CPU load level. The feature rejects new digital calls (PRI, CAS, and ISDN), with minor disruption to system users.

Link Fragmentation and Interleaving

Large data packets can adversely delay delivery of small voice packets, reducing speech quality. Fragmenting these large data packets into smaller ones and interleaving voice packets among the fragments reduces jitter and delay. The Cisco IOS Link Fragmentation and Interleaving (LFI) feature helps satisfy the real-time delivery requirements of VoIP.

Note For more information about Cisco LFI, refer to Voice over IP Quality of Service for Low-Speed PPP Links at the following URL:
http://www.cisco.com/warp/public/788/voice-qos/voip-mlppp.html

Traffic Engineering Guidelines

The following topics discuss additional traffic-engineering challenges posed by a Cisco ASAP Solution network, the majority of which are related to varying bandwidth throughout the network:

- Challenges with Low-Speed Links (<1.5 Mbps)
- Gateway with High-Speed Egress Interface
- Gateway with Low-Speed Egress Interface
- Edge Router with High-Speed Egress Interfaces
- Core Issues
- Optimizing the Performance of the Cisco SC2200

Challenges with Low-Speed Links (<1.5 Mbps)

With bandwidth under T1 rates, extra attention must be paid to preventing voice quality from suffering. With respect to voice/voice and voice/data contention, the remedies in Table 4-1 on page 4-3 apply here. However, two new challenges arise in low-speed links and must be dealt with:

- Packet Residency
- Bandwidth Consumption

Packet Residency

Packet residency, also known as serialization delay, is the term for the effect large data packets have on voice quality. Data packets can be so large that the time it takes to transmit one large packet over a low-speed WAN link can exceed the voice delay budget. Interleaving mechanisms break large data packets into smaller ones, so that small voice packets can be inserted, or interleaved, between data fragments to ensure timely voice transport. The Cisco Multilink Point-to-Point Protocol (MLP) feature, and more recently the Cisco Multichannel Multilink PPP (MMP) feature, is designed to do this. (See Configuring Multilink PPP, page 4-34.)

Bandwidth Consumption

Managing bandwidth consumption is a top priority over low-speed links. Techniques include the use of low-bit-rate audio codecs, RTP (Real-Time Transport Protocol) header compression, and voice activity detection (VAD). VAD detects periods of silence and prevents “empty” packets from being transmitted during those periods.

Other Bandwidth and Core Related Issues

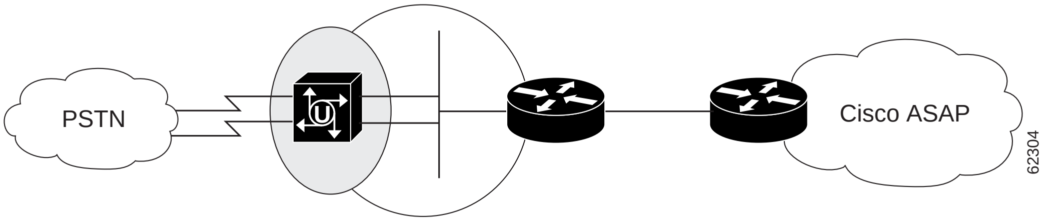
This section discusses additional issues, related to the following topics:

- Gateway with High-Speed Egress Interface
- Gateway with Low-Speed Egress Interface
- Edge Router with High-Speed Egress Interfaces
- Edge Router with Low-Speed Egress Interfaces
- Core Issues

Gateway with High-Speed Egress Interface

Figure 4-2 highlights a UG with a high-speed egress interface. Refer to Table 4-5 on page 4-16 for remedies to be applied.

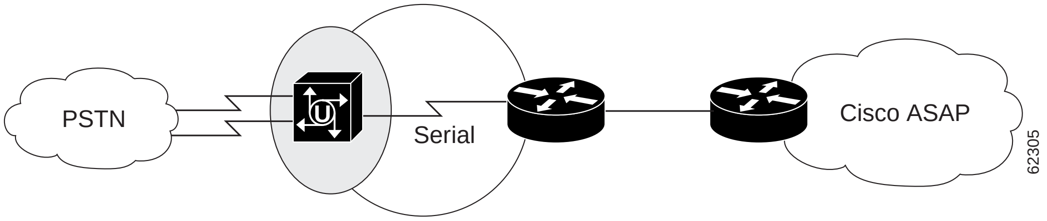
Figure 4-2 Gateway with High-Speed Egress Interface



Gateway with Low-Speed Egress Interface

Figure 4-3 highlights a UG with a low-speed egress interface. Refer to Table 4-5 on page 4-16 for remedies to be applied.

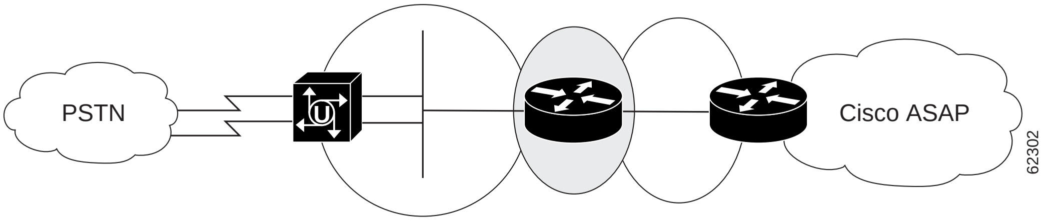
Figure 4-3 Gateway with Low-Speed Egress Interface



Edge Router with High-Speed Egress Interfaces

Figure 4-4 highlights an edge router with high-speed egress interfaces. Refer to Table 4-5 on page 4-16 for remedies to be applied.

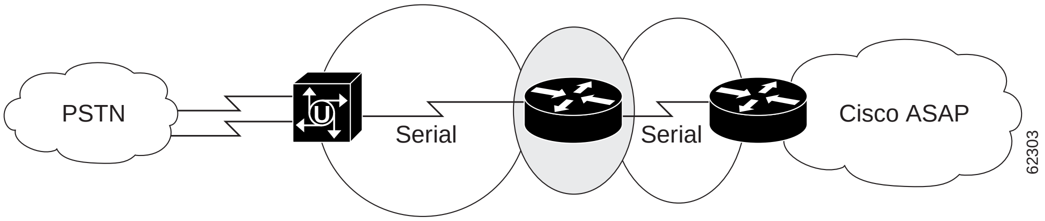
Figure 4-4 Edge Router with a High-Speed Egress Interface



Edge Router with Low-Speed Egress Interfaces

Figure 4-5 highlights an edge router with low-speed egress interfaces. Refer to Table 4-5 on page 4-16 for remedies to be applied.

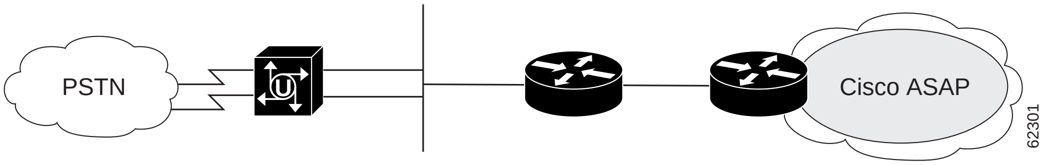
Figure 4-5 Edge Router with Low-Speed Egress Interfaces



Gateway with High-Speed Egress Interface

Figure 4-6 highlights a UG with a high-speed egress interface. Refer to Table 4-5 on page 4-16 for remedies to be applied.

Figure 4-6 Gateway with High-Speed Egress



Core Issues

Table 4-5 lists the issues related to bandwidth and the network core, with recommended remedies.

Table 4-5 Bandwidth and Core Related Issues and Remedies

Components	Issue	Description	Features to Enable/Remedy
UG	High-speed egress	WAN connection between PSTN UG and edge router; see Figure 4-2	• Enhanced CAC • IP precedence
	Low-speed egress	Serial connection between PSTN UG and edge router; see Figure 4-3	• Enhanced CAC • IP precedence • RSVP • RSVP-based CAC • LLQ • RSVP/LLQ integration • LFI scheme • Compression
Edge router	High-speed egress interfaces	WAN connection between edge router and (1) Cisco ASAP network and (2) PSTN UG; see Figure 4-4	• RSVP[1] • LLQ • RSVP/LLQ integration[2]
	Low-speed egress interfaces	Serial connection between edge router and (1) Cisco ASAP network and (2) PSTN UG; see Figure 4-5	• RSVP[1] • LLQ[2] • RSVP/LLQ integration[2] • LFI scheme • Compression
Cisco ASAP core	Congestion	Any link that can become congested through a combination of signaling, voice, and data traffic; see Figure 4-6	• LLQ • Do not oversubscribe. • Ensure RSVP in access network restricts voice traffic on entrance to core.

[1] Assuming voice/voice contention is enabled and device is IP aware.

[2] Assuming device is IP aware and supports LLQ.

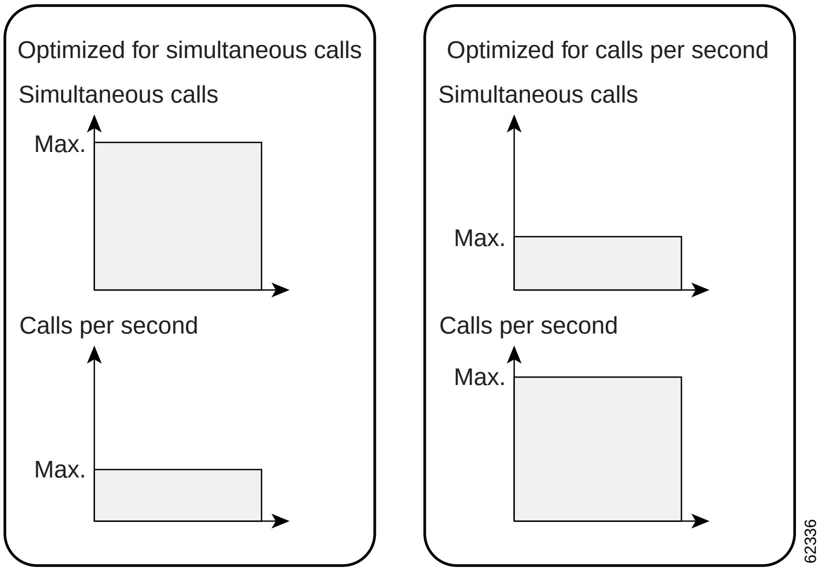
Optimizing the Performance of the Cisco SC2200

Figure 4-7 illustrates two optimization models for SS7 interconnect. One is optimized for simultaneous calls, the other for calls per second (CPS).

Caution This discussion is a general discussion to illustrate the trade-offs involved. There are a variety of issues related to optimizing traffic on a Cisco SC2200 node, and you should always consult with your Cisco account representative regarding best practices and to ensure that traffic availability is not impaired.

In most cases, however, optimizing for CPS will be sufficient.

Figure 4-7 Two Optimization Models: Simultaneous Calls and Calls per Second



L2TP Tunneling and VPDNs

As background to the following abbreviated discussion, refer to Layer 2 Tunnel Protocol at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120t/120t1/l2tpt.htm

Note A Cisco 7200 VXR series router is the broadband services aggregator platform that serves as the L2TP network server, or LNS. (For a brief introduction to L2TP tunneling and the Cisco LNS, refer to Cisco L2TP Network Server in Chapter 3, "Solution Components," of the *Cisco ASAP Solution Overview and Planning Guide* at the following URL: http://www.cisco.com/univercd/cc/td/doc/product/access/solution/asap/index.htm

Refer also to L2TP Network Server, page 5-5, for installation and related information.

The document Layer 2 Tunnel Protocol illustrates the relationship between what is referred to as the LAC, or local access concentrator, and the LNS. The LAC is essentially the NAS, or in our case a UG. VPDN commands are used in conjunction with commands to enable AAA. The LNS can be a Cisco AS5000 series UG, but larger networks may require a Cisco 7200 or Cisco 7400 series.

To create a VPDN, or virtual private data (or dial) network, you must do the following on both the UG and the LNS:

- Before Configuring the LAC or LNS
- Configuring VPDN on the LAC
- Configuring VPDN on the LNS

Note The following is only a brief summary of essential steps. Refer to the document Layer 2 Tunnel Protocol for details, including extended debug examples and troubleshooting tips.

Before Configuring the LAC or LNS

Do one of the following before configuring the LAC (UG) or LNS for VPDN using L2TP:

- Configure VPDN with local authentication by using the **hostname** command to assign a user identity (*user@domain.com*) and verify peer-to-peer connectivity.
- Configure security attributes by using AAA, TACACS+, or RADIUS, and confirm peer-to-peer connectivity before configuring the LAC and LNS for VPDN. The example below uses AAA.

Configuring VPDN on the LAC

In the following basic example, a dial subscriber accesses the LAC through an ISP or the PSTN. The UG, in turn, communicates with the LNS through an L2TP tunnel. Complete the following procedures:

- Perform Global LAC Configuration
- Edit LAC VPDN Parameters

Note For an overview and details of configuring virtual private networks (VPN), refer to the chapter "Configuring Virtual Private Networks" in the *Cisco IOS Dial Technologies Configuration Guide, Release 12.2*, at the following URL:
http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fdial_c/index.htm

Perform Global LAC Configuration

The following steps are done in global configuration mode.

Step 1 Enable AAA globally.

```
aaa new-model
```

Step 2 Enable AAA authentication for PPP, and use the default method of PPP authentication.

```
aaa authentication ppp default local
```

Step 3 Enable VPDN.

Note In VPDN configuration mode the prompts vary according to the **vpdn-group** subcommands, as illustrated below.

```
LAC(config)# vpdn enable
```

Step 4 Define a VPDN group. Here we create group 1.

```
LAC(config)# vpdn-group 1
```

Any groups defined on the LAC must also be defined on the LNS. See Edit LNS VPDN Parameters, page 4-22.

Edit LAC VPDN Parameters

You can begin the following while still in global configuration mode.

Step 1 To configure VPN tunnel authentication, you need to establish an L2TP password (tunnel secret), a tunnel name of the UG (optional), and the other UG's tunnel name and the tunnel secret as a user name (optional). This is done in global configuration and addresses the *vpdn-group*.

a. Here we address the vpdn-group we just established.

```
LAC(config)# vpdn-group 1
```

Note Technically, the UG is now functioning in its role as a local access concentrator, or LAC, as is reflected in the prompt. The name of the UG will be the name you have established for it. To illustrate the role of this gateway, our hostname is *LAC* for the following example

The following is done in VPDN configuration mode, which changes to *request-dialin* mode (*config-vpdn-req-dialin*) to reflect the fact that we are configuring the access gateway.

Step 2 Allow the UG to respond to dialin requests from a given IP address and domain.

a. Enable the UG to request either L2F or L2TP dialin requests. Note how the prompt changes.

```
LAC(config-vpdn)# request-dialin
```

The prompt will change to reflect the fact that we are configuring the request side of the tunnel.

b. Specify which tunneling protocol is to be used. Here we select L2TP.

```
LAC(config-vpdn-req-in)# protocol l2tp
```

Note Because dialin requests will originate from this platform, the prompt changes to indicate this (*req-in*).

You must select a protocol before you can establish a tunnel secret and tunnel name.

c. Specify the domain name of the users that are to be tunneled. Here our domain is **cisco.com**.

```
LAC(config-vpdn-req-in)# domain cisco.com
```

d. (Optional) Instead of using a domain, you can specify the DNIS number of users that are to be tunneled.

```
LAC(config-vpdn-req-in)# dnis <dnis number>
```

Note You can configure multiple domain names or DNIS numbers for an individual *request-dialin* subgroup.

e. Now you will need to exit this configuration mode to proceed.

```
LAC(config-vpdn-req-in)# exit
```

Step 3 Specify the IP address that the UG will use to establish the tunnel. This is the IP address of the tunnel server.

```
LAC(config-vpdn)# initiate-to <IP address>
```

Step 4 Configure the tunnel secret and tunnel name.

a. Configure the tunnel secret.

```
LAC(config-vpdn)# l2tp tunnel password <tunnel-secret>
```

b. (Optional) Configure the tunnel name of the LAC.

```
LAC(config-vpdn)# local name <tunnel-name>
```

Note By default, the UG uses the *hostname* as the tunnel name in VPN tunnel authentication. However, you can configure a local name for the VPN (VPDN) group. In negotiating VPN tunnel authentication for this VPN group, the UG will use the local name as the tunnel name.

c. (Optional) Configure the other UG's tunnel name and the tunnel secret as the username.

```
LAC(config-vpdn)# username <tunnel-name> password <tunnel-secret>
```

Note This configures a tunnel name and tunnel secret as the LNS's username/password combination. The tunnel secret must be the same on both platforms. Each UG must have the other's tunnel name (specified by either the **hostname** or **local name** command) configured as a username, with the tunnel secret as the password. If the other UG uses the **l2tp tunnel password** command to configure the tunnel secret, the optional commands are not necessary. However, the tunnel secret *must be the same* on both UGs.

Step 5 (Optional) You can specify the method used to determine whether a dialin call should be tunneled. The syntax is as follows:

```
LAC(config-vpdn)# vpdn search-order { domain | dnis | domain dnis | dnis domain }
```

If both keywords are entered, the UG will search the criteria in the order in which they are entered.

Tip Optionally, you can also configure a maximum number of connections that this VPN group will support, as well as the priority of the group. Use the command option **limit** for the former, and the command option **priority** for the latter.

Step 6 To complete the configuration, proceed to Configuring VPDN on the LNS.

Configuring VPDN on the LNS

The following basic example configures VPDN on the L2TP network server (LNS), or host (also referred to as the tunnel server). The establishment of the username and password is not shown. This is very similar (and parallel) to Configuring VPDN on the LAC, page 4-18. Complete the following procedures:

- Perform Global LNS Configuration
- Edit LNS VPDN Parameters

Perform Global LNS Configuration

The following steps are done in global configuration mode. Here we also create a virtual template on the LNS.

Step 1 Enable AAA globally.

```
aaa new-model
```

Step 2 Enable AAA authentication for PPP, and use the default method of PPP authentication.

```
aaa authentication ppp default local
```

Step 3 Create a virtual template corresponding to the VPDN group, and assign all values for virtual access interfaces.

a. Create the virtual template.

```
interface virtual-template <number>
```

New interfaces, as they are assigned, will copy (clone) the attributes of the virtual template to create virtual access interfaces. (There is no correspondence between the virtual template and the VPDN group.)

b. Borrow the IP address from interface ethernet 1.

```
ip unnumbered <interface-type><number>
```

Note As with a physical interface, we could use, for example, **ip unnumbered Ethernet0**. The virtual access interfaces will use the IP address of this interface.

c. Use CHAP to authenticate PPP.

```
ppp authentication chap
```

Step 4 Disable multicast fast switching (recommended).

```
no ip mroute-cache
```

Step 5 Enable VPDN.

Note In VPDN configuration mode the prompts vary according to the **vpdn-group** subcommands, as illustrated below.

```
LNS(config)# vpdn enable
```

Step 6 Define a VPDN group. Here we create group 1, corresponding to what we defined on the LAC.

```
LNS(config)# vpdn-group 1
```

Edit LNS VPDN Parameters

Begin the following while still in global configuration mode.

Step 1 Address the vpdn-group that has been established.

```
LNS(config)# vpdn-group 1
```

The following is done in VPDN configuration mode, which changes on the LNS to *accept-dialin* mode (*config-vpdn-acc-dialin*), to reflect the fact that we are configuring the tunnel server.

Step 2 Allow the LNS to respond to dialin requests from a given IP address and domain.

a. Enable the LAC to request either L2F or L2TP dial-in requests. Note how the prompts change.

```
LNS(config-vpdn)# accept-dialin
```

b. Specify which tunneling protocol is to be used. Here we select L2TP, to conform with the the protocol on the UG.

```
LNS(config-vpdn-acc-in)# protocol l2tp
```

Note Because dialin requests will terminate at this platform, the prompt changes to indicate this (*acc-in*).

c. Specify the number of the virtual template to be used to clone the virtual access interface.

```
LNS(config-vpdn-acc-in)# virtual-template <number>
```

The number will be the same as that established in Perform Global LAC Configuration, page 4-18.

d. Now you will need to exit this configuration mode to proceed.

```
LNS(config-vpdn-acc-in)# exit
```

Step 3 Configure the tunnel secret and tunnel name. These must be the same as those established on the LAC.

a. Configure the tunnel secret.

```
LNS(config-vpdn)# l2tp tunnel password <tunnel-secret>
```

b. (Optional) You can specify that the tunnel server will identify itself with a local name. Otherwise, the server will identify itself with its hostname.

```
LNS(config-vpdn)# local name <tunnel-name>
```

c. (Optional) Configure the other UG’s tunnel name and the tunnel secret as the username.

```
LNS(config-vpdn)# username <tunnel-name> password <tunnel-secret>
```

Note If the LAC uses the **l2tp tunnel password** command to configure the tunnel secret, the optional commands are not necessary. However, the tunnel secret must be the same on both the LAC and the LNS.

Step 4 Instruct the LNS to accept tunnels from LACs that have the following hostname configured as a local name.

```
LNS(config-vpdn)# terminate-from <hostname>
```

Note The above method is suitable to smaller networks, but not to networks of any substantial size. Larger networks commonly make use of AAA servers to provide authentication.

Enabling Cisco RPMS 1.x

This section is primarily a detailed discussion of the configuration required on the UG in its function as a NAS in support of dial services. To install and configure a Cisco RPM server, refer to Cisco Resource Pool Manager Server, page 5-7.

This discussion addresses Cisco RPMS prior to Release 2.0. Refer to Cisco Resource Pool Manager Server 1.1 at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/access/acs_soft/rpms/rpms_1-1/index.htm

See also Enabling Local RPM, page 2-32.

Caution In initial releases of the Cisco ASAP Solution, Cisco RPMS supports dial services only. In subsequent releases, Cisco RPMS 2.0 will be used, and multivendor management support will be provided through nonproprietary RADIUS.

Overview

There are five principle components to enabling a UG to interact with a Cisco RPMS:

- Configuring AAA support
- Configuring TACACS+ support
- Configuring resource pooling (see Caution below)
- Configuring VSA support
- Enabling VPDN (optional)

Caution Cisco recommends that you define all relevant entities before actually turning resource pooling on. This will prevent calls from being redirected by this feature before the configuration is complete.

Required Activities

The required configuration activities, in the recommended sequence, are as follows:

1. Define an AAA server group of Cisco RPMSs.
2. Enable multithreaded AAA processing.
3. Define the Cisco RPMS TACACS+ servers.
4. Define the source interface for TACACS+.
5. Enable resource pooling to the Cisco RPMS.
6. Enable additional accounting attributes.

7. Define resource groups.
8. Enable resource pooling.
9. Enable administrative updates to the Cisco RPMS.
10. Limit the peak call rate.
11. Enable VSAs in accounting records.

Optional Activities

There are two optional activities:

- Enabling VPDN (Optional)
- Configuring SGBP (Optional)

Tip For a brief summary see Summary of Key Steps, page 4-29.

The following topics are also presented in this section:

- Enabling VPDN (Optional)
- An Example UG-to-RPMS Configuration
- Useful Troubleshooting Commands
- SS7 Resource Groups
- An Example SS7 Resource Group

Basic Configuration

Step 1 Define an AAA server group of Cisco RPMSs.

Use the following syntax to define an AAA server group of Cisco RPM servers.

a. Ensure that the following command is issued on the UG. It may already be present.

```
aaa new-model
```

Caution You must issue the command **aaa new-model** in order to enter any aaa commands.

b. Assign a name to the AAA server group.

```
aaa group server tacacs+ <name>
```

where *name* is local to the UG but must match the *name* defined in Step 5, Enable resource pooling to the Cisco RPMS., page 4-25.

c. Assign a hostname and IP address to the AAA server.

```
server <hostname/ipaddress>
```

d. Add an entry for each Cisco RPMS with which the UG will communicate. The first server listed becomes the primary Cisco RPMS.

Note In a cluster architecture, define a primary Cisco RPMS first (first server line). Then define a master/backup Cisco RPMS server (second server line) for redundancy, in case the primary Cisco RPMS fails.

Step 2 Enable multithreaded AAA processing.

The enabling of multithreaded processing for AAA transactions can be considered essential, to keep transaction latency at a minimum. The simple syntax is as follows.

```
aaa process <n>
```

where *n* is an integer that determines the number of AAA processes.

Note the following suggestions and caveats.

- Use *n* less than or equal to 30 for RPMS 1.1 deployments.
- Increase the value of *n* to decrease the PPP queue.
- Use the command **show ppp queue** to check for improvements.
- Ensure that the CPU is not affected by PPP queue improvements.
- Use this command *with care*, as it creates a bell-curve performance profile that is environment specific.

Step 3 Define the RPMS TACACS+ servers.

You must configure a **tacacs-server** definition for each RPMS listed under the AAA server group. See Step 1, Define an AAA server group of Cisco RPMSs., page 4-24.

Use the following syntax to define a Cisco RPM server.

```
tacacs-server host <hostname/ipaddress> key <string>
```

where *string* is an identifying keyword.

Note The key *must* match the shared secret defined for this UG on the RPMS.

Step 4 Define the source interface for TACACS+.

The source IP address used for TACACS+ packets from the UG must match that configured in the RPMS or that returned by a name server lookup.

Use the following syntax to define a source interface.

```
ip tacacs source-interface <interface>
```

where *interface* is typically a loopback interface that ensures there is no dependence on a physical interface being up.

Step 5 Enable resource pooling to the Cisco RPMS.

Use the following syntax to enable resource pooling to the Cisco RPM server.

```
resource-pool aaa protocol group <name>
```

where *name* is a link to the AAA group defined in Step 1, Define an AAA server group of Cisco RPMSs., page 4-24.

Note AAA must be enabled on the UG through the command **aaa new-model** in order for this command to be entered.

Note If you have configured SS7 Interconnect on the UG, predefined SS7 resource groups are automatically created on the UG once this command is configured. See SS7 Resource Groups, page 4-31.

Step 6 Enable additional accounting attributes.

VSAs provide additional information for PPP accounting records, such as overflow flags, customer profile matches, and so on.

Use the following syntax to enable additional accounting attributes. Here we associate PPP accounting with the resource pool.

```
resource-pool aaa accounting ppp
```

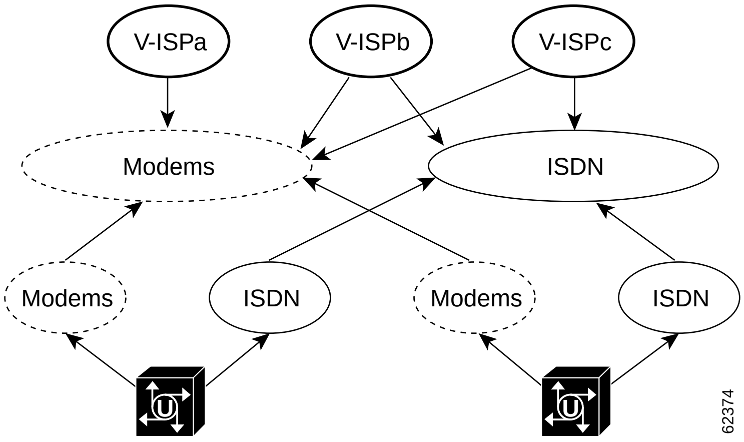
See also Enable VSAs in accounting records., page 4-28.

Note For more information on AAA accounting and VSAs, refer to Understanding and Provisioning AAA Billing in Chapter 3, "Provisioning Shared Support Services," of the *Cisco Wholesale Voice Solution Design and Implementation Guide*, at the following URL: http://www.cisco.com/univercd/cc/td/doc/product/access/sc/rel7/soln/wv_rel1/wvpg/index.htm

Step 7 Define resource groups.

Each UG contributes resources to common pools. Customers then access the pooled resources through RPMS. Figure 4-8 illustrates virtual resource groups (for virtual ISPs) across multiple access servers (UGs in our case). Resource groups on individual UGs must have the same names.

Figure 4-8 Virtual Resource Groups Serving Virtual ISPs



Do the following to define resource groups.

a. Giving thought to your network design and requirements, determine resource group names as appropriate. Table 4-6 lists resource types, both port-based and non-port-based.

Table 4-6 Resource Types for Defining Resource Groups (Port-Based and Non-Port-Based)

Port-Based	Non-Port-Based
Modems	HDLC framers (for ISDN synchronous calls)
V.110	V.120
Defined by slot/port range	Defined by size of group

b. Use the following syntax to define a resource group:

Note This substep is not required (or supported) if the UG is configured for SS7 interconnect, in which case port ranges are assigned automatically. See SS7 Resource Groups, page 4-31.

```
resource-pool group resource <name>
```

where *name* is used by the RPMS to reference resources available on the UG. Resource groups of the same name must be created on the RPMS for them to be used. Resource groups with the same name allow the pooling of those resources across multiple UGs.

c. Use the following example syntax to define port-based resources, which are referenced according to their physical location.

```
range port <shelf/slot/port> <shelf/slot/port>
```

Port location format is platform dependent, and may also be *slot/port*. In this example the two *shelf/slot/port* values define the beginning and end of a range. Noncontiguous ranges can be defined by separate **range port** statements. Note the following example:

```
resource-pool group resource modems
 range port 1/4/0 1/4/143
 range port 1/6/0 1/6/143
```

Note Where SS7 interconnect is used, these port ranges do not need to be defined. Ports are assigned dynamically.

d. Use the following syntax to define a non-port-based resource group:

```
resource-pool group resource <name>
range limit <n>
```

where *n* is an integer that does not exceed the number of HDLC framers on the UG. Note the following example:

```
resource-pool group resource modems
 range limit 256
```

e. Adhere to the following resource group guidelines:

- Ensure that there are no overlaps. Port-based resources can exist in *only one* resource group.
- Use the same name for the same resource group types across all access servers. If the UGs are to go into the same virtual resource pool across all UGs, the resource group name must be the same on each UG that is to be pooled. (However, you may have predefined resource groups if you are using Cisco RPMS and SS7 interconnect.)

- Use the same names on the UGs as you use on Cisco RPMS. The names used on the UGs in a pool must match exactly with the names assigned on the server.

Step 8 Enable resource pooling.

Now you are ready to turn resource pooling on. To do so before completing the configuration would cause calls to be redirected unnecessarily through this feature, with undesirable consequences.

To enable resource pooling, use the following global configuration command:

```
resource-pooling enable
```

Step 9 Enable administrative updates to the Cisco RPMS.

You must enable the UG to send administrative updates to the Cisco RPMS. Use the following syntax to enable administrative updates.

```
tacacs-server administration
```

Caution This command is *essential*. Without it, the UG and RPMS will not stay in sync. However, do *not* enter this command if resource pooling is not enabled. If you disable resource pooling (**resource-pooling disable**, or **no resource-pooling enable**), be sure to disable this command *first* (**no tacacs-server administration**).

Step 10 Limit the peak call rate.

You can limit the peak call rate by defining the maximum depth of the resource monitor queue. Use the following syntax to limit the peak call rate.

```
resource-pool throttle <n> <cause-code>
```

where

- *n* is an integer from 1 to 1600
- *cause-code* is either (1) an integer from 1 to 27 or (2) the keyword *default*
- the keyword *default* returns “REQ_CHANNEL_NOT_AVAILABLE”

The UG will reject calls if the number of calls in the resource monitor queue reach the throttle limit set by *n*.

Step 11 Enable VSAs in accounting records.

Now you must enable VSA processing on the UG. This is essential to sending VSAs (including such items as overflow flags) to the Cisco RPMS. See Enable additional accounting attributes., page 4-26.

Use the following syntax to enable VSAs on the UG.

```
radius-server vsa send accounting
```

The above is used in conjunction with AAA accounting and AAA server definitions defined in previous steps.

Note For more information on AAA accounting and VSAs, refer to Understanding and Provisioning AAA Billing, in Chapter 3, “Provisioning Shared Support Services,” of the *Cisco Wholesale Voice Solution Design and Implementation Guide*, at the following URL:
http://www.cisco.com/univercd/cc/td/doc/product/access/sc/rel7/soln/wv_rel1/wvpg/index.htm

Summary of Key Steps

The following summarizes the preceding steps:

```
aaa group server tacacs+ <name>
 server <hostname/ipaddress>
aaa process <n>
tacacs-server host <hostname/ipaddress> key <string>
ip tacacs source-interface <interface>
resource-pool aaa protocol group <name>
resource-pool aaa accounting ppp
resource-pool group resource <name> <---see Note below
 range port <location-start> <location-end>
 range limit <x>
resource-pooling enable
tacacs-server administration
resource-pool throttle <n> <cause-code>
radius-server vsa send
```

Note This is not enabled if the UG is enabled for SS7 interconnect.

Enabling VPDN (Optional)

You can configure VPDN information on an RPMS or an AAA server. Use the following command:

```
vpdn enable
```

Note This is also discussed in Local VPDN, page 2-15.

This is the only configuration required if the RPMS provides VPDN definitions. VPDN definitions may also be provided by an AAA server. However, a VPDN check is always made to the Cisco RPMS first.

Configuring SGBP (Optional)

If more than one home gateway is specified, sessions are load-balanced in “round-robin” fashion among the IP addresses, in which the next available address is used in series. For Multilink PPP (MLP) connections as are used in ISDN, half of the packets will be lost. With SGBP (Stack Group Bidding Protocol), the UG is configured to belong to groups of peers called *stack groups*. All members of a stack group are peers, and therefore do not need a permanent “lead” UG.

After a connection is established with one member of a stack group, that member owns the call. If a second call comes in from the same client and a different UG answers the call, the first UG establishes a VPDN tunnel and forwards all packets belonging to the call to the (new) UG that owns the call.

Note Configuring SGBP is also discussed in Enabling Multichassis Multilink PPP, page 2-14.

For an illustration of this issue and configuration information, refer to Configuring Stack Group Bidding Protocol at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/access/acs_soft/rpms/rpms_1-0/rpmsconf/app_sgbp.htm

An Example UG-to-RPMS Configuration

```
<---snip--->
!aaa group server tacacs+ RPMS
 server 172.19.50.122
 server 172.19.50.125
!
aaa processes 20
!
<---snip--->
!
resource-pooling enable
!
resource-pool group resource modems
 range port 1/4/0 1/4/143
 range port 1/6/0 1/6/143
!
resource-pool group resource ISDN
 range limit 256
!
resource-pool aaa accounting ppp
resource-pool aaa protocol group RPMS
<---snip--->a
!
ip tacacs source-interface FastEthernet0/1
!
<---snip--->
!
vpdn enable
!
<---snip--->
!
tacacs-server host 172.19.50.122 key vt-lab
tacacs-server host 172.19.50.125 key vt-lab
tacacs-server administration
!
<---snip--->
!
radius-server vsa send accounting
<---snip--->
```

Useful Troubleshooting Commands

The following **show** commands provide a variety of resource pool information.

- **show resource-pool resource**—Provides a list of all configured resources on the UG, including modem and ISDN resources.
- **show resource-pool resource** *name*—Provides detailed information on the named resource group. The following is example output.

```
ASAP_UG#show resource-pool resource modems
144 resources in the resource group
8 resources currently active
248 calls accepted in the resource group
0 calls rejected due to resource unavailable
0 calls rejected due to resource allocation errors
never since last clear command
```

SS7 Resource Groups

Predefined SS7 resource groups are automatically created when resource pooling is enabled to a Cisco RPMS from a UG that is configured for SS7 interconnect. (See Enable resource pooling to the Cisco RPMS., page 4-25). An SS7 resource group is created for each call type that can be terminated on that system. The maximum number of resources that are available for each call type are placed in the associated resource group.

The following message will appear to indicate the resource groups have been created successfully:

```
SS7/RPM/RPMS are all configured and the predefined resource groups will be created
```

When SS7 interconnect is enabled on the UG, resource groups are defined, and the following command is issued:

```
resource-pool aaa protocol group <name>
```

the following error message will be displayed:

```
"You must remove all the configured resource group(s) and re-enter this command for
SS7/RPM/RPMS interworking"
```

To remedy this, delete any defined resource groups on the UG and then reenter the command.

Table 4-7 lists the current predefined SS7 resource groups. Their types are self-explanatory.

Table 4-7 Predefined SS7 Resource Groups

SS7 Resource Group
rg_ss7_mica
rg_ss7_nextport
rg_ss7_digital
rg_ss7_v110
rg_ss7_v120

Caution Note the following restrictions and caveats.

- You *cannot* change the names of these resource groups.
- You *can* delete both the groups and some or all resources within them. However, you must remove any call types you do not want to support.
- You *cannot* add any additional resource groups. An attempt to create an additional resource group will result in the following error message:

  ```
  res-group <name> cannot be created/modified when SS7/RPM/RPMS are all enabled
  ```

Table 4-8 lists the default RPMS SS7 resource group mappings.

Table 4-8 Default SS7 Resource Group Mappings

RPMS SS7 Resource Groups	Default Mapping to UG SS7 Resource Groups
rg_ss7_rpms_speech	rg_ss7_nextport rg_ss7_mica
rg_ss7_rpms_digital	rg_ss7_digital
rg_ss7_rpms_v110	rg_ss7_nextport rg_ss7_mica
rg_ss7_rpms_v120	rg_ss7_v120

An Example SS7 Resource Group

The following is an example of an SS7 resource group.

```
resource-pool group resource rg_ss7_digital
 range limit 192
!
resource-pool group resource rg_ss7_v120
 range limit 192
!
resource-pool group resource rg_ss7_nextport
 range port 2/0 2/107
 range port 3/0 3/107
 range port 4/0 4/107
 range port 5/0 5/107
 range port 6/0 6/107
 range port 7/0 7/107
```

Enabling Cisco AR

Cisco Access Registrar 1.7 is the most recent version of the Cisco AR access policy server, and is documented at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cnsar/1_7/

It is beyond the scope of the current document to detail the provisioning of the Cisco AR server.

Note The Cisco ASAP Solution does not preclude the use of other AAA servers, including those of third parties.

Refer to the following documents for the details of understanding and using Cisco AR:

- *Cisco Access Registrar 1.7 Installation and Configuration Guide*
- *Cisco Access Registrar 1.7 Concepts and Reference Guide*
- *Cisco Access Registrar 1.7 Release Notes*
- *Cisco Access Registrar 1.7 User’s Guide*

Overview of Authentication and Authorization on the Cisco AR

The following brief overview provides basic information about how Cisco Access Registrar (AR) performs the basic RADIUS functions of authentication and authorization as defined in Internet RFC 2865. An understanding of the process can be helpful in troubleshooting.

Authentication and authorization are defined as follows.

- **Authentication**—determining the identity of a user of a client NAS or UG through user identification and password validation and deciding whether to grant access
- **Authorization**—determining the level of network services available to authenticated users after a connection has been established

Note For a discussion of the third component of AAA, accounting, refer to Understanding and Provisioning AAA Billing in Chapter 3, "Provisioning Shared Support Services," of the *Cisco Wholesale Voice Solution Design and Implementation Guide*, at the following URL:
http://www.cisco.com/univercd/cc/td/doc/product/access/sc/rel7/soln/wv_rel1/wvpg/index.htm

Basic Authentication and Authorization

The Cisco AR server provides authentication and authorization service to clients that are network access servers (UGs in the case of the Cisco ASAP Solution). The following paragraphs describe the steps to a connection.

1. The process begins when a user dials into the UG and enters a user name and a password. The UG creates an Access Request containing attributes such as the user's name, the user's password, the ID of the client, and the port ID that the user is accessing.
2. The AR server determines which hardware (client UG) sent the request, parses the packet, and determines whether to accept the request. The AR server checks to see if the client's IP address is listed in the server's directory */Radius/Clients/<Name>/<IPAddress>*.
3. After accepting the request, the AR server does the following:
   a. Sets up the Request Dictionary based on the packet information.
   b. Runs any incoming scripts (user-written extensions to Cisco AR).

      An incoming script can examine and change the attributes of the request packet or the environmental variables that can affect subsequent processing. On the basis of default values or scripts, the AR server chooses a service to authenticate and authorize the user.

   c. Directs the request to the appropriate service, which then performs authentication or authorization according to the type specified in the server directory */Radius/Services/<Name>/<Type>*.
   d. Performs session management, directing the request to the appropriate Session Manager.
   e. Performs resource management for each Resource Manager in the Session Manager. The AR server directs the request to the appropriate resource manager listed in the server directory */Radius/SessionManagers/<Name>/<ResourceManagers>/<Name>*.

      The resource manager then allocates or checks the resource according to the type listed in */Radius/<ResourceManagers>/<Name>/<Type>*.

4. The AR server finally creates and formats an Access Accept, Access Reject, or Access Challenge response, then sends it to the client UG.

Using Cisco RLM

Cisco Redundant Link Manager (RLM) provides virtual link management over multiple IP networks, so that the Q.931 signaling protocol and other proprietary protocols can be transported on top of multiple redundant links between a Cisco Signaling Controller (in our case the Cisco SC2200) and a network access server (in the case of the Cisco ASAP Solution, the UG). RLM provides the following features:

- Opens, maintains, and closes multiple links
- Manages buffers of queued signaling messages
- Monitors whether links are active (for link failover and SC failover)

The user can create more than one IP connection between the SC and the UG.

For more information, including related documents, configuration examples, and RLM commands, refer to Redundant Link Manager (RLM), at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/access/acs_serv/as5400/sw_conf/ios_121/pull_rlm.htm

Configuring Multilink PPP

Multilink PPP

Multilink PPP (MLP) allows a single end-system to split and recombine packets across a logical pipe (or *bundle*) that is formed by multiple links. MLP provides bandwidth on demand and reduces transmission latency across WAN links.

For the details of configuring MLP, refer to Configuring Media-Independent PPP and Multilink PPP at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/dialts_c/dtsprt4/dcdppp.htm

Multichassis Multilink PPP

Multichassis Multilink PPP (MMP) improves on MLP by allowing links to terminate on multiple routers with different remote addresses. This feature, which accommodates both analog and digital traffic, is intended for large pools of dial-in users, where a single chassis cannot provide enough dial ports. In particular, ISPs can allocate a single ISDN rotary number to several ISDN PRIs across several routers, providing easy expansion and scalability, assured fault tolerance, and redundancy. MMP allows UGs to be stacked together and appear as a single gateway; if one UG fails, another in the stack can accept calls.

For the details of configuring MMP, refer to Configuring Multichassis Multilink PPP at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/dialns_c/dnsprt1/dcdmppp.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.

Note Traps supported will vary according to the IOS release. For a listing of SNMP traps supported up through Cisco IOS Software version 12.1(3)T, refer to Cisco IOS SNMP Traps Supported and How to Configure Them at the following URL:
http://www.cisco.com/warp/public/477/SNMP/snmp_traps.html

A current list of all supported Cisco IOS Software Simple Network Management Protocol (SNMP) trap Object Identifiers (OIDs) can be at the following URL:
ftp://ftp.cisco.com/pub/mibs/oid/

The basic configuration required on the UG to support SNMP is presented in Enabling SNMP on the Gateway, page 2-37. For additional details of configuring SNMP, refer to Configuring SNMP Support at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/ffun_c/fcfprt3/fcf014.htm

Also see Task 3. Enabling SNMP, at the following URL:

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

For a list of Management Information Bases (MIBs) for use with SNMP, see Using MIBs, page 4-35.

Caution Cisco recommends that you enable SNMP on all UGs. 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 MIBs

MIBs, or Management Information Bases, are databases of network performance information (the characteristics and parameters of network devices) for use by a variety of management applications. SNMP is a commonly used protocol for defining the information types in a MIB.

Table 4-9 lists some useful Cisco MIBs that support the Cisco ASAP Solution.

Table 4-9 Useful Cisco MIBs that Support the Cisco ASAP Solution

Dial (Modem) MIBs	Voice MIBs
DIAL-CONTROL-MIB	CISCO-VOICE-DIAL-CONTROL-MIB
CISCO-DIAL-CONTROL-MIB	CISCO-CAS-IF-MIB
CISCO-POP-MGMT-MIB	CISCO-VOICE-IF-MIB
CISCO-MODEM-MGMT-MIB	CISCO-VOICE-NUMBER-EXPANSION-MIB
	CISCO-CALL-APPLICATION-MIB
	CISCO-SIP-UA-MIB

Obtaining MIBs

To obtain Cisco MIBs, as well as application notes related to their use, refer to Cisco MIBs at the following URL:

http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

Using MIB Locator

A convenient tool, MIB Locator, lets users browse an automated database of MIBS. A component of Cisco Feature Navigator (for which you will need a Cisco account password), MIB Locator provides a wider range of information to help the user maintain and troubleshoot networks. To use MIB Locator, follow the instructions below.

Step 1 Go to the following URL:

http://www.cisco.com/go/fn

Step 2 Enter a Cisco password as requested. The Feature Navigator window appears.

Step 3 In the left-hand frame, click MIB Locator. The MIB Locator window appears.

You can search for MIBs by using the following criteria:

- Release
- Platform family
- Feature set
- Image name
- Specific MIB name

Step 4 Use the criteria you want, then click the **Submit** button to issue your request.

You will be asked to narrow your search until you find the specific MIB you want. You can both view and download specific MIBs.

CHAPTER 5

Establishing Solution Components

This chapter provides links to online information needed to install and use the varied components of the Cisco ASAP Solution, including the latest information on IOS features and caveats. The following topics are presented:

- Establishing H.323 Core Components
- Establishing SS7 Signaling Components
- Establishing Cisco Catalyst Switches
- Establishing Management and Shared Support Services

Note For a background on the components discussed in this chapter, refer to *Cisco ASAP Solution Overview and Planning Guide*, available at the following URL: http://www.cisco.com/univercd/dd/td/doc/product/access/solution/asap/index.htm

Establishing H.323 Core Components

The equipment you need for a Cisco ASAP Solution may already be installed in your network. For the latest information on installing and configuring components of the H.323 gatekeeper core, including release notes, refer to the URLs listed in this chapter.

Tip Not all the components listed below provide full mixed voice and data services, but the links are useful references to equipment you may already have installed.

Core components consist of the following:

- Gateways
- Gatekeepers and Directory Gatekeepers

Gateways

The following equipment can be used as either H.323 gateways or (in the case of dial-only services) as NASs. The term universal gateway, or UG, is used to apply to components that have universal ports in support of mixed dial and voice services.

Note Cisco AS5300 GWs are not part of the Cisco ASAP Solution insofar as they are not universal gateways, although they can be used to support dial-only services. In initial releases of the Cisco ASAP Solution, the Cisco AS5850 supports dial only.

The following also applies to the same devices when they are used as NASs (network access servers) in dial applications.

Cisco AS5350

Refer to Cisco AS5350 at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/access/acs_serv/as5350/index.htm

Installing Universal Gateway Cards

To install UG cards (also known as universal port cards), refer to *Cisco AS5350 Universal Gateway Card Installation Guide* at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/access/acs_serv/as5350/hw_inst/53crd/index.htm

Configuring Cisco IOS Software

To configure Cisco IOS software, and learn about feature modules, refer to *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

Managing Port Services

To manage port services, refer to Managing Port Services on the Cisco AS5350 Universal Gateway at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/access/acs_serv/as5350/sw_conf/alxnxpt.htm

Also refer to *Managing Port Services Command Reference* at the following URL:

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

Cisco AS5400

Refer to Cisco AS5400 at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/access/acs_serv/as5400/index.htm

Installing Universal Gateway Cards

To install UG cards, refer to *Cisco AS5400 Universal Gateway Card Installation Guide* at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/access/acs_serv/as5400/hw_inst/mig/index.htm

Configuring Cisco IOS Software

To configure Cisco IOS software, and learn about feature modules, refer to *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

Managing Port Services

To manage port services, refer to Managing Port Services on the Cisco AS5400 Universal Gateway at the following URL:

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

Also refer to *Managing Port Services Command Reference* at the following URL:

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

Cisco AS5800

Refer to Cisco AS5800 at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/access/acs_serv/as5800/index.htm

Cisco AS5850

Refer to Cisco AS5850 at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/access/acs_serv/as5850/index.htm

Note In initial releases of Cisco ASAP Solution, the Cisco AS5850 supports dial services only. Refer to *Cisco ASAP Solution Release Notes* for the most current information.

Installing Universal Gateway Cards

To install UG cards, refer to *Cisco AS5850 Universal Gateway Card Guide* at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/access/acs_serv/as5850/hw_inst/5850cg/index.htm

Configuring Cisco IOS Software

To configure Cisco IOS software, refer to Cisco AS5850 Universal Gateway Commissioning Guidelines at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/access/acs_serv/as5850/sw_conf/comm.htm

Operations, Administration, Maintenance, and Provisioning

For OAM&P information related to the Cisco AS5850, refer to *Cisco AS5850 Universal Gateway Operations, Administration, Maintenance, and Provisioning Guide* at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/access/acs_serv/as5850/sw_conf/5850oamp/index.htm

Managing Port Services

For detailed information on managing port services, refer to Managing Port Services on the Cisco AS5850 Universal Gateway (see preceding Note) at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121limit/121x/121xv/121xv_5/portserv/fthybrid.htm

Also refer to *Managing Port Services Command Reference* at the following URL:

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

Gatekeepers and Directory Gatekeepers

The following equipment can be used as both GKs and DGKs. Installation and instructions, as well as the latest release notes, are available at the URLs listed below.

⚠ **Caution** The Cisco 3620 is not suitable for this purpose. For reasons of performance, Cisco recommends that you use the Cisco 3640 when the gatekeeper must manage fewer than 100 subscribers.

Cisco 3640, Cisco 3660

Refer to Cisco 3600 Series Routers at the following URL:

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

Cisco 7202

Refer to Cisco 7202 at the following URL:

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

Cisco 7204

Refer to Cisco 7204 at the following URL:

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

Cisco 7206

Refer to Cisco 7206 at the following URL:

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

Establishing SS7 Signaling Components

Where SS7 signaling is required (the most common case), the Cisco ASAP Solution relies on the Cisco SS7 Interconnect for Voice Gateways Solution. For the most current documentation on the signaling link termination systems needed to implement SS7 signaling, refer to Cisco SS7 Interconnect for Voice Gateways Solution, Release 1.3, at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/access/sc/rel7/soln/voip13/index.htm

Note Refer to *Cisco ASAP Solution Release Notes* for the latest version of software required, as well as for additional important information.

Establishing Cisco Catalyst Switches

Cisco Catalyst switches, both Cisco Catalyst 5000 and 6000 series, are optional but useful adjuncts to managing a Cisco ASAP Solution network.

Caution Cisco recommends that you use Cisco Catalyst 6000 series switches, to ensure the best QoS for voice services. Switches are also managed components of a Cisco SC2200 node. Among the Cisco Catalyst 5000 series switches, only the Cisco Catalyst 5500 switch has been tested with Cisco CMNM. Cisco 6000 series switches cannot currently be managed by means of Cisco CMNM.

Refer to Cisco 6000 Family Switches at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/index.htm

Establishing Management and Shared Support Services

The applications required for your particular implementation will vary, and different applications provide different features.

Network Timing

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

For more information, refer to Providing Network Timing through NTP in Chapter 2, “Provisioning the Gatekeeper Core,” of the *Cisco Wholesale Voice Solution Design and Implementation Guide* at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/access/sc/rel7/soln/wv_rel1/wvpg/index.htm

L2TP Network Server

For installation and configuration information, as well as related documents, refer to Cisco 7200 VXR at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/core/7200vx/

Note The Cisco 7200 VXR is a different product from the Cisco 7200 family routers, insofar as it requires a different Cisco IOS image.

Cisco Universal Gateway Manager

For a quick start, user's guide, and release notes, refer to Cisco Universal Gateway Manager (UGM) at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/ugm/index.htm

Caution For Cisco UGM to work properly, the correct SNMP traps must be established on the GW so they can be processed.

Note Cisco UGM 1.0 can support two traps per second, or five traps per second in a 5-minute burst window. See the section Network Configuration Scenario in the Release Notes at the above URL.

CiscoWorks2000 Voice Manager

Cisco recommends 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

Additional useful information, including a discussion of managing dial plans, is available under CiscoWorks2000 Voice Manager 2.0 at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/voicemgr/cvm20/

Cisco MGC Node Manager

For information in installing and configuring Cisco MGC Node Manager (CMNM) 1.5, refer to *Cisco Media Gateway Controller Node Manager User's Guide 1.5* at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/access/sc/rel8/cmnmgr/

See also Establishing Cisco Catalyst Switches, page 5-5.

Cisco Voice Services Provisioning Tool

Cisco Voice Services Provisioning Tool (VSPT) can be used as an integrated component of the Cisco MGC Node Manager (see above), or as a standalone application.

For further information about Cisco VSPT, refer to Cisco Voice Services Provisioning Tool v1.5 at the following URL:

http://www.cisco.com/warp/public/cc/pd/ga/sc/prodlit/vsptv_ds.htm

Note When used with Cisco MGC Node Manager, Cisco VSPT is launched directly from a Cisco CMNM menu.

Cisco Info Center

The most current release of Cisco Info Center (CIC) is 3.0.1. For installation instructions and additional information, refer to Cisco Info Center 3.0.1 Release at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/info_ctr/3_0_1/index.htm

Cisco Internetwork Performance Monitor

For installation instructions, a user guide, and additional information, refer to Internetwork Performance Monitor, Release 2.3, at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/ipmcw2k/cipm23/index.htm

Cisco Access Registrar

The recommended version of Cisco Access Registrar (AR) is Release 1.7. Refer to Cisco Access Registrar 1.7 at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cnsar/1_7/

Note in particular the following documents:

- *Cisco Access Registrar 1.7 Installation and Configuration Guide*
- *Cisco Access Registrar 1.7 Release Notes*

Cisco Resource Pool Manager Server

For initial releases of the Cisco ASAP Solution the recommended version of Cisco Resource Pool Manager Server is Release 1.1. For installation and configuration instructions, a solutions guide, and the latest information, refer to Cisco Resource Pool Manager Server 1.1 at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/access/acs_soft/rpms/rpms_1-1/index.htm

Note Later versions of the Cisco ASAP Solution will require Cisco RPMS Release 2.0. That release of Cisco RPMS is referred to as Cisco Resource Policy Management Server.

IVR Services

For a discussion of how to implement IVR services, including Cisco TCL IVR, refer to Provisioning Services to Support IVR, in Chapter 3, “Provisioning Shared Support Services,” in the *Cisco Wholesale Voice Solution Design and Implementation Guide* at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/access/sc/rel7/soln/wv_rel1/wvpg/index.htm

Billing Systems for Calling Card Services

For a discussion of how to implement billing systems for calling card services, refer to Establishing Billing Systems for Calling Card Services, in Chapter 3, “Provisioning Shared Support Services,” in the *Cisco Wholesale Voice Solution Design and Implementation Guide* (see the URL referred to immediately above).

Note Cisco Billing and Measurements Server (BAMS) is also available as a component within Cisco MGC Node Manager. Refer to Billing and Measurements Server Phase 2 at the following URL: http://www.cisco.com/univercd/cc/td/doc/product/access/sc/bams2/index.htm

Caution BAMS is still under test in the Cisco ASAP Solution. If you are using BAMS to provide billing data and are upgrading to Cisco ASAP Solution 1.0, take care to monitor your billing data for accuracy.

APPENDIX A

AAA Method Lists

Method lists are significant features of AAA, and it is important to understand their syntax and use. The following AAA method lists are discussed in this appendix:

- AAA Authentication Method Lists
- AAA Authorization Method Lists
- AAA Accounting Method Lists

AAA Authentication Method Lists

AAA authentication method lists control administrative access and authentication. Consider the following general rules when applying authentication method lists:

- A definition is required for each subset of each AAA element that you want to support.
- You can define a sequence of methods, which will be attempted in the order in which they are listed.

⚠ **Caution** It is possible for you to lock yourself out of the system, so BEWARE!

Authentication Services

Table A-1 lists and describes commonly defined AAA authentication services.

Table A-1 Commonly Defined AAA Authentication Services

Service	Description
enable	Enables access at privileged command level
login	Authenticate only if user is not already authenticated
ppp	Enables PPP

Types of Authentication Lists and Methods

You can also use either *named* or *default* method lists. Use named method lists if you want to use different method lists for the same services but on different interfaces. Named lists are typically used to discriminate between *remote user* login to the system and *administrative* login. Default method lists simply use the word **default** as a name keyword.

Caution If you do not apply a named list to an interface or interfaces, it will not be used. Also, the **name** option does not appear in the syntax related to applying named lists under the interfaces.

Table A-2 lists and defines AAA authentication methods.

Table A-2 AAA Authentication Methods

Method	Definition
group *name*	Use a specified AAA group
if-needed	Authenticate only if user is not already authenticated
local	Use local username lookup
local-case	Use case-sensitive local username lookup
none	Do not authenticate (See Caution below)

Caution For security reasons, take care in using the **none** option.

Order of Authentication Lists

In general, if a “fail” response is received, authentication attempts will not continue down the list. However, there are exceptions to this: one is when an error is received (for example, a server is down); the other is during a local username lookup. In addition, the authentication list will continue if there is not a match to an entry in the local username list. If there is a match in the local list, but authenticatio fails (the password is wrong), the authentication will not continue.

Caution Take great care in defining lists. Consider possible server-failure scenarios, and minimize repeated authentications.

Authentication Syntax

The syntax for AAA authentication is as follows:

aaa authentication *service listname method1 method2* . . . *methodn*

where *service* represents available services that are predefined; *listname* can be either a user-defined character string or the keyword **default**; and the methods are lists of predefined options in combination with reference to named AAA groups where the **group** option is used.

AAA Authorization Method Lists

AAA authorization method lists control authorization for various services. Consider the following general rules when applying authorization method lists:

- A definition is required for each subset of each AAA element that you want to support.
- You can define a sequence of methods, which will be attempted in the order in which they are listed.

Authorization Services

Table A-3 lists and describes commonly defined AAA authorization services. Other services include commands and reverse Telnet. See Enabling AAA and RADIUS, page 2-25.

Table A-3 Commonly Defined AAA Authorization Services

Service	Description
exec	Starts an EXEC shell, used with scripted logins and TCP Clear
network	Enables related network services, such as PPP

Types of Authorization Lists and Methods

You can also use either *named* or *default* method lists, as discussed in Types of Authentication Lists and Methods, page A-2. Remember to apply the list to an interface.

Table A-4 lists and defines AAA authorization methods.

Table A-4 AAA Authorization Methods and Their Definitions

Method	Definition
group *name*	Use a specified AAA group
if-authenticated	Let users who are successfully authenticated do whatever they want
local	Use the local database
local-case	Use case-sensitive local username lookup
none	Let users do whatever they want (See Caution below)

⚠ **Caution** For security reasons, take care in using the **none** option.

Order of Authorization Lists

In general, if a “fail” response is received, authorization attempts will not continue down the list. However, an exception is when a server is down.

Caution Take great care in defining lists, and consider possible server failure scenarios.

Authorization Syntax

The syntax for AAA authorization is as follows:

aaa authorization *service listname method1 method2 . . . methodn*

where *service* represents available services that are predefined; *listname* can be either a user-defined character string or the keyword **default**; and the methods are lists of predefined options in combination with reference to named AAA groups where the **group** option is used.

AAA Accounting Method Lists

When AAA accounting is activated, the UG reports user activity to a TACACS+ or RADIUS server (depending on what is implemented) in the form of accounting records. The data, stored as attribute-value (AV) pairs can then be analyzed for network management, client billing, or auditing.

AAA accounting method lists control administrative access and authentication. Consider the following general rules when applying authentication method lists:

- A definition is required for each subset of each AAA element that you want to support.
- You can define a sequence of methods, which will be attempted in the order in which they are listed.

Accounting Services

Table A-5 lists and describes commonly defined AAA accounting services.

Table A-5 Commonly Defined AAA Accounting Services

Service	Description
enable	Enables access at the priveleged command level
login	Enables login access, either through scripted login of telnet
ppp	Enables PPP

Types of Accounting Lists and Methods

You can also use either *named* or *default* method lists. Use named method lists if you want to use different method lists for the same services but on different interfaces. Named lists are typically used to discriminate between *remote user* login to the system and *administrative* login. Default method lists simply use the word **default** as a name keyword.

Caution If you do not apply a named list to an interface or interfaces, it will not be used. Also, you can only use the default method list for system accounting.

Table A-6 lists and defines AAA accounting methods.

Table A-6 AAA Accounting Methods and Their Definitions

Method	Definition
broadcast	Broadcast accounting records
group *name*	Send accounting records to a specified AAA group

You will also need to determine when to send accounting records, through time command options that are entered in the accounting method list. Table A-7 lists and defines the time options for AAA accounting.

Table A-7 AAA Accounting Time Options and Their Definitions

Option	Definition
start-stop	Send both start and stop records
stop-only	Send only stop records
wait-start	Same as for **start-stop**, but wait for the ACK of the start record before allowing the user session to proceed

Order of Accounting Lists

Accounting records will be sent to subsequent defined methods only if no ACK is received. This indicates that an error is received, for example, a server is down.

Accounting Syntax

The syntax for AAA accounting is as follows:

aaa accounting *service listname method1 method2* . . . *methodn*

where *service* represents available services that are predefined; *listname* can be either a user-defined character string or the keyword **default**; and the methods are lists of predefined options in combination with reference to named AAA groups where the **group** option is used.

APPENDIX B

Format C

Format C is not an industry standard, but is the format used by Ascend Communications applications. Cisco developed Format C to support Cisco customers requiring a format like that that used by Ascend platforms.

Format C provides output in machine-friendly format, using a 16-bit binary field. The bits and the facility locations they represent are as follows.

15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
Shelf		Slot				Port					Channel				

For example, a NAS-Port value of 54 (binary 110110) represents serial 1:22, as shown below>

15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
										1	**1**	**0**	**1**	**1**	**0**

You can also assign Format C for all attributes, as follows:

```
radius-server attribute nas-port format c
```

Note Ascend Communications is now part of Lucent Technologies. However, you can still find useful information at http://www.ascend.com/, by searching for "Ascend."

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
AR	Cisco Access Registrar
ASAP	Cisco Any Service, Any Port solution
ASP	application service provider

B

BAMS	Cisco Billing and Measurements Server

C

CAC	call admission control
CBWFQ	class-based weighted fair queueing
CDR	call detail record
CEF	Cisco Express Forwarding
CHAP	Challenge Handshake Authentication Protocol
CIC	Cisco Info Center; carrier identification code
CLI	command line interface
CLID	Calling Line IDentification
CO	central office
CPU	central processing unit
CVM	CiscoWorks2000 Voice Manager

D

dCEF	Distributed Cisco Express Forwarding
DGK	directory gatekeeper
DNIS	Dialed Number Identification Service

E

EMEA	Europe, Middle East, and Africa
EMS	element management system
EO	end office

F

FG	feature group

G

GK	gatekeeper
GW	gateway

H

HDLC	high-level data link control
HSRP	Hot Standby Router Protocol—used to ensure GK fault tolerance

I

ICMP	Internet Control Message Protocol
ICPIF	ITU G.113 Calculated Planning Impairment Factor
IETF	Internet Engineering Task Force
IMT	intermachine trunk
IPM	Cisco Internetwork Performance Monitor
IS	in service
ISP	Internet service provider
ISUP	ISDN User Part
ITSP	Internet telephony service provider
ITU	International Telecommunication Union
IVR	interactive voice response

L

L2F	Layer 2 Forwarding Protocol
L2TP	Layer 2 Tunneling Protocol
LAC	L2TP access concentrator
LFI	Cisco Link Fragmentation and Interleaving
LLQ	low latency queuing
LNS	L2TP network server

M

MGC	Media Gateway Controller
MGCP	Media Gateway Control Protocol
MIB	Management Information Base
MLP	Multilink PPP
MML	Man-Machine Language

MMP	Multichassis Multilink PPP
MTP	Message Transfer Part

N

NAS	network access server
NMS	network management system
NTP	Network Time Protocol
NFAS	Non-Facility Associated Signaling

O

OGW	originating gateway
OLO	other local operator; other licensed operator
OOS	out of service
OPC	origination point code
OPT	Open Packet Telephony
OSP	Open Settlements Protocol
OSS	Operations Support System

P

PCM	pulse code modulation
PDF	Portable Document Format
PIN	personal identification number
POP	point of presence
PPM	port policy management
PPP	Point-to-Point Protocol
PSQM	perceptual speech quality measure
PSTN	public switched telephone network
PTT	Post, Telephone, Telegraph—a government-mandated or -operated national telephony carrier

Q

QoS	quality of service
QoV	quality of voice (SNMP)

R

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
RLM	Cisco Redundant Link Manager
RPM	resource pool management; resource pool manager
RPMS	Cisco Resource Policy Management Systgem (formerly Cisco Resource Pool Manager Server)
RSVP	Resource Reservation Protocol
RTCP	Real Time Conferencing Protocol; RTP Control Protocol
RTP	Real-Time Transport Protocol
RTR	Response Time Reporter

S

SC	signaling controller—a Cisco SC2200 signaling gateway that converts SS7 to a backhauled NI-2 protocol to gateways; see also VSC and MGC
SGBP	Stack Group Bidding Protocol
SGCP	Simple Gateway Control Protocol
SLIP	Serial Line Internet Protocol
SLT	signaling link termination; Cisco Signaling Link Terminal—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
SPE	system processing engine
SS7	Signaling System 7

T

TAC	Technical Assistance Center
TACACS	Terminal Access Controller Access Control System
TCL	Tool Command Language
TDM	time-division multiplex; time-division multiplexing
TFTP	Trivial File Transfer Protocol
TGW	terminating gateway

U

UG	universal gateway
UGM	Cisco Universal Gateway Manager
URL	uniform resource locator

V

VPDN	virtual private data (or dial) network
VPN	virtual private network
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

WFQ	weighted fair queuing
WIC	WAN interface card

INDEX

Symbols

- &F command 2-44
- &W command 2-44

A

- AAA
  - accounting method lists A-4
  - administrative accounting method list 2-29
  - administrative authentication method list 2-28
  - administrative authorization method list 2-28
  - administrative command level 2-28
  - administrative options 2-28
  - authentication method lists A-1
  - authorization method lists A-3
  - defining servers 2-26
  - enabling on gateway 2-26
  - method lists 2-25
  - methods 2-25
  - server group 4-24
  - server groups 2-26
- aaa accounting command A-5
- AAA accounting time options and their definitions (table) A-5
- aaa authentication command A-2
- AAA authentication methods (table) A-2
- aaa authorization command A-4
- AAA authorization methods and their definitions (table) A-3
- aaa group command 4-24
- AAA methods and their definitions (table) A-3, A-5
- aaa nas-port extended command option 2-31
- aaa new-model command 2-26, 4-18, 4-24
- aaa preauth command 2-34
- aaa process command 4-25
- Access Accept 4-33
- Access Challenge 4-33
- access control lists 2-41
- Access Reject 4-33
- Access Request 4-33
- accounting 4-33
  - enabling for prepaid 2-21
  - H.323 for voice 2-25
  - method list 2-27
- Accounting Session ID 2-31
- acct-port 2-30
- Acct-Session-Id string 2-31
- ACLs 2-41
- Adobe Acrobat
  - using xiii
- alternate dial peers 4-10
- AR 5-7
- Ascend port format 2-31
- async mode interactive command 2-12
- AT command 2-44
- Attribute 25 2-31
- Attribute 26 2-31
- Attribute 44 2-31
- authentication 4-33
  - administrative method list 2-28
  - method list 2-26
- authorization 4-33
  - administrative method list 2-28
  - method list 2-26
- auth-port 2-30

autobusyout feature 4-5

autoselect during-login command 2-13

B

BAMS 5-8

bandwidth and core related issues and remedies (table) 4-16

bandwidth reservation 4-8

B-channel 2-8

- configuring negotiation 2-24

bearer-cap 3100Hz command 2-51

bearer-cap command 2-51

best-effort service 4-8

billing

- systems 5-8

busy command 4-7

busyout command option 4-5

C

CAC 2-35

- commands for enhanced features 4-4
- managing contention 4-3
- RSVP-based 4-2
- setting resource threshold on UG 2-35

cache

- aging 2-42
- settings 2-42

call fallback active command 4-10

call fallback command 4-9

call fallback monitor command 4-10

call fallback threshold delay loss command 4-10

call fallback threshold icpif command 4-10

Calling Line IDentification 2-34

call-number command option 4-7

call rate restriction 4-7

call rsvp-sync command 4-8

call spike command 4-7

call spikes 2-35

call threshold 2-35

call threshold command 2-35, 4-5, 4-6

call thresholds 2-35

call threshold trigger options (table) 4-6

CallTracker 2-36

- configuring 2-38

calltracker command 2-38

call treatment 2-35, 4-6

- cause code 4-7
- on OGW 4-6
- on TGW 4-7

call treatment command 2-35, 4-6

call type 2-34

call types and rejection criteria (table) 4-3

call waiting 2-48

call-waiting survival 2-48

cause code 4-7

cause code 49 4-8

cause-code command 4-7

cause codes 2-36

CBWFQ 4-11

CEF 2-42

CIC 5-7

Cisco 2611 SLT 3-2

Cisco 3600 Series 5-4

Cisco 7200 4-17

Cisco 7200 VXR 5-5

Cisco 7200 VXR series 4-17

Cisco 7202 5-4

Cisco 7204 5-4

Cisco 7206 5-4

Cisco 7400 4-17

Cisco access patforms and recommended CEF and cache settings (table) 2-42

Cisco Access Registrar 4-32, 5-7

Cisco AR 3-4

Cisco AS5300 xi, 3-2, 5-2

Cisco AS5350 5-2

Cisco AS5400 5-2

Cisco AS5800 xi, 5-3

Cisco AS5850 5-3

Cisco ASAP Solution

defined xi

Cisco Billing and Measurements Server 5-8

Cisco Call Admission Control Based on CPU Utilization feature 4-12

CISCO-CALL-APPLICATION-MIB 4-36

CISCO-CAS-IF-MIB 4-36

Cisco Catalyst 5000 series 5-5

Cisco Catalyst 5500 switch 5-5

Cisco Catalyst 6000 series 5-5

Cisco Catalyst switches 5-5

Cisco CMNM 5-6

CISCO-DIAL-CONTROL-MIB 4-36

Cisco Express Forwarding 2-42

Cisco Feature Navigator 4-36

Cisco Info Center 5-7

Cisco Internetwork Performance Monitor 5-7

Cisco IOS Link Fragmentation and Interleaving (LFI) feature 4-12

Cisco LNS 4-17

Cisco Low Latency Queuing (LLQ) feature 4-11

Cisco MGC Node Manager 5-6

CISCO-MODEM-MGMT-MIB 4-36

Cisco Multichannel Multilink PPP (MMP) feature 4-13

Cisco Multilink PPP (MLP) feature 4-13

CISCO-POP-MGMT-MIB 4-36

Cisco PSTN Fallback feature 4-9, 4-10

Cisco Redundant Link Manager 4-34

Cisco Resource Reservation Protocol (RSVP) feature 4-11

Cisco Resource Unavailable Signaling feature 4-5

Cisco RLM 2-9

Cisco RPMS 2-15, 2-33, 3-1, 3-4, 5-7

configuring gateway for 2-16

Cisco RSVP Support for Low Latency Queuing feature 4-12

Cisco SC2200

performance optimization and trade-offs 4-17

Cisco SC2200 node 3-2

CISCO-SIP-UA-MIB 4-36

Cisco SS7 Interconnect for Access Gateways Solution 3-1

Cisco SS7 Interconnect for Voice Gateways Solution 3-2

Cisco T.38 Fax Relay for Universal Gateways feature 2-21

Cisco TCL IVR 5-7

Cisco Universal Gateway Manager 5-6

CISCO-VOICE-DIAL-CONTROL-MIB 4-36

CISCO-VOICE-IF-MIB 4-36

CISCO-VOICE-NUMBER-EXPANSION-MIB 4-36

Cisco Voice Services Provisioning Tool 5-6

Cisco VoIP CAC with RSVP feature 3-3

Cisco VoIP Call Admission Control using RSVP feature 4-2

Cisco Wholesale Voice Solution Overview 1-1

CiscoWorks2000 Voice Manager 5-6

CLID 2-34

clock-period 2-7

cloning 2-45

cluster architecture 4-25

CMNM 5-6

codec G711ulaw command 2-51

commonly defined AAA accounting services (table) A-4

commonly defined AAA authentication services (table) A-1

commonly defined AAA authorization services (table) A-3

components

establishing 1-2

config-gateway command 4-4

Configuring Media Gateways for the SS7 Interconnect for Voice Gateways Solution 2-34

congestion 4-16

console logging

disabling 2-2, 2-6, 2-40

contention 4-3

controller
  E1 2-4
  T1 2-4, 2-5
  T3 2-5, 2-6
controllers
  configuring 2-4
  configuring for NFAS 2-8
CPS 4-16
CT3 2-22

D

dCEF 2-42
D-channel 2-5, 2-9
debugging 2-2, 2-6
default SS7 resource group mappings (table) 4-32
delay 2-48, 4-9, 4-13
delay command option 4-9
DIAL-CONTROL-MIB 4-36
Dialed Number Identification Service 2-22
dialer dnis group command 2-34
dialer-group command 2-13
dialer idle-timeout command 2-12
dialer interface 2-13
dialer pool command 2-13
dialer rotary-group command 2-14
dial-in interfaces (lines)
  configuring 2-12
dial-in modem service 2-12
dial peer
  alternate 4-10
  configuring on UG 2-18
  for TDM switching 2-23
  POTS 2-18
  prepaid calling-card services 2-19
  VoIP 2-18
dial-peer voice command 2-22
dial plan 3-2
  and number normalization 2-17
  static 2-18
  unified 2-17
dial service
  configuring asynchronous 2-12
  configuring synchronous 2-13
dial services
  categories 2-11
  configuring modem 2-11
direct-inward-dial command 2-19
directory gatekeeper 3-4
distributed CEF 2-42
distributed keyword 2-42
DNIS 2-22, 2-34
  assigning DNIS groups 2-34
documentation
  conventions xiv
  release of xi
domain command 4-19
drop and insert 2-22

E

E1
  configuring controller 2-4
E1 R2 2-4
echo analysis 2-49
echo cancellation 2-48
  disabling 2-49
  typical settings 2-50
echo-path tail delay 2-48
edge router with high-speed egress interfaces (figure) 4-15
edge router with low-speed egress interfaces (figure) 4-15
enable community string (SNMP) 2-37
encapsulation ppp command 2-13

BETA DRAFT - CISCO CONFIDENTIAL - 4/11/2002, 14:35:22

F

fallback 4-10

fall through to dial 2-17

FastEthernet interface 2-3

fax

configuriong 2-21

T.38 Fax for Cisco Universal Gateways

reference 2-21

fax protocol command 2-21

fax rate disable command 2-51

figures

Edge Router with High-Speed Egress Interfaces 4-15

Edge Router with Low-Speed Egress Interfaces 4-15

Gateway with High-Speed Egress Interface 4-14

Gateway with Low-Speed Egress Interface 4-14

Sliding Windows Applied to Monitor Number of Incoming Calls 4-8

Two Optimization Models: Simultaneous Calls and Calls per Second 4-17

Virtual Resource Groups Serving Virtual ISPs 4-26

Format C 2-31, B-1

G

G.168 2-49

gateway

defined 2-1

gateway with high-speed egress interface (figure) 4-14

gateway with low-speed egress interface (figure) 4-14

glare 2-24

glare (B-channel) 2-8

grooming 2-22

group-async interface 2-12

configuring 2-12

H

H.245 2-21

H.323 4-11

accounting for voice 2-25

configuring registration on gateway 2-19

H.323 SETUP message 4-8

hairpin command 4-6

hairpinning 4-6

header compression 4-13

HGW 2-15

high-speed egress (interfaces) 4-16

home gateway 2-15

hostname command 4-18

hunt (SS7 to PRI) 2-23

hunt group 2-23

I

ICPIF 4-9

Response Time Reporter 4-9

thresholds 4-9

icpif command option 4-9

ICPIF values (table) 4-9

impairment

factor 4-9

initiate-to command 4-20

interface

cloning 2-45

FastEthernet 2-3

precloning 2-45

serial 2-7

TACACS+ 2-3

virtual access 2-45

virtual template 2-45

interface-type 2-3

interleaving 4-13

io-cache enable command 2-42

ip cache-ager command 2-42
IP network delay 2-48
IP precedence 4-11
ISDN
  B-channel 2-8
  D-channel 2-5
  PRI 2-7
  switch type 2-7, 2-8
isdn negotiate-bchan resend-setup command 2-13
isdn-reject command 4-7
ISDN signaling
  configuring D-channels on UG 2-9
IVR 2-20
  configuring on UG 2-20

L

L2F 2-15
L2TP
  Layer 2 Tunnel Protocol
    reference 4-17
  network server 4-17
L2TP network server 2-15
L2TP tunnel 2-15
LAC 2-15, 4-17
level
  command 2-28
  command option 2-28
  privilege 2-28
LFI 4-12
link fragmentation and interleaving 4-12
listnames 2-28
LLQ 4-1, 4-10, 4-11
LNS 2-15, 4-17
load-interval command 2-13
logging 2-2, 2-6, 2-37
  disabling 2-2, 2-6
  disabling console logging 2-40
logging command 2-37, 2-41
loopback interface 2-3
loss command option 4-9
low-speed egress (interfaces) 4-16
LZJH compression algorithm 2-47

M

Mail Transport Agents 2-3
method lists
  accounting (AAA) A-4
method lists (AAA) A-1, A-3
MIB
  CISCO-CALL-APPLICATION-MIB 4-36
  CISCO-CAS-IF-MIB 4-36
  CISCO-DIAL-CONTROL-MIB 4-36
  CISCO-MODEM-MGMT-MIB 4-36
  CISCO-POP-MGMT-MIB 4-36
  CISCO-SIP-UA-MIB 4-36
  CISCO-VOICE-DIAL-CONTROL-MIB 4-36
  CISCO-VOICE-IF-MIB 4-36
  CISCO-VOICE-NUMBER-EXPANSION-MIB 4-36
  DIAL-CONTROL-MIB 4-36
MIB Locator 4-36
Microsoft NetMeeting
  noncompliance with T.38 fax relay 2-18, 2-21, 2-50, 3-3
MLP 4-13, 4-29, 4-34
MMP 2-14, 4-34
modem
  configuring recovery 2-43
  defining capability 2-43
  failure and recovery 2-42
  initialization script 2-43
  recovery 2-42
modemcap 2-43
modem dialin command 2-13, 2-47
modem features
  V.44 2-47

V.92 2-47
modem-on-hold 2-47
MOH 2-47
mta command 2-3
MTAs 2-3
multichassis multilink PPP 2-10, 2-14
multilink PPP 2-10
multithreaded AAA processing 2-28
multithreaded processing 4-25

N

nas port attribute 2-27
NFAS 2-5
configuring controllers for 2-8
no-qos command 4-7
no-resource command 4-7
no use-proxy command 2-51
NTP 2-7, 5-5
NTP server 2-7
ntp update-calendar command 2-7
number normalization 3-2

O

OIDs 4-35
optimization 2-39
access lists 2-41
CPU 2-39
CPU efficiency 2-39
delaying trunk activation 2-46
disabling PPP multilink fragmentation 2-41
enabling passive header compressoin 2-46
line configuration for dial 2-47
modems 2-42
port resources 2-40
preventing process takeover 2-41
processes 2-40
scaling AAA processing 2-41
SNMP 2-44
suppressing modem tests 2-44
system logging 2-40
using CEF 2-42
virtual access interfaces 2-45

P

packet
loss 4-9
residency 4-13
PDF xiii
playmsg command 4-7
ports
managing port services 5-4
PPM
enabling RADIUS-based 2-34
enablling on gateway 2-32
ppp multilink command 2-13
preauthentication 2-34
precloning 2-45
predefined SS7 resource groups (table) 4-31
prepaid
accounting 2-21
enabling billing services 2-20
PRI
configuring 2-5
ETSI 2-4
NI2 2-4
priority queuing 4-11
probe 4-10
protocol command 4-19, 4-22
PSTN fallback 4-4, 4-9, 4-10

Q

Q.931

+/IP 4-11
DISCONNECT message 4-8
signaling 2-10
QC 2-47
QoS
basic steps to implementing 4-2
CAC 4-2
RSVP 4-2
QoS unavailable 4-8
quick connect 2-47

R

RADIUS
command reference 2-30
command syntax 2-29
defining basic server attributes on gateway 2-30
enabling on gateway 2-29
radius-server command 2-30
radius-server vsa send authentication command 2-31
RAI 2-35, 4-4
range port command 4-27
RAS 3-2
rate-limit command option 2-41
reject command 4-7
reporting 2-36
request dialin command 4-19
Request Dictionary 4-33
resource groups 2-9, 4-26
Resource Manager 4-33
resource monitor queue 4-28
resource pool 2-32, 4-26
establishing profile 2-33
resource-pool command 2-32, 4-26
resource pooling 4-28
resource threshold 2-35
resource threshold command 4-4
resource types 4-26
resource types for defining resource groups (port-based and non-port-based) (table) 4-27
Response Time Reporter 4-9
resv-timer command option 4-8
reverse Telnet A-3
rg_ss7_digital 4-31, 4-32
rg_ss7_mica 4-31, 4-32
rg_ss7_nextport 4-31, 4-32
rg_ss7_rpms_digital 4-32
rg_ss7_rpms_speech 4-32
rg_ss7_rpms_v110 4-32
rg_ss7_rpms_v120 4-32
rg_ss7_v110 4-31
rg_ss7_v120 4-31, 4-32
RLM 2-10, 4-34
groups 2-10
NFAS group 2-23
rlm-group number 2-10
RPM 2-33
enabling on gateway 2-33
reference 2-33
RSVP 4-2, 4-8, 4-11
RSVP-based CAC 4-3
RTCP 4-11
RTP 4-10, 4-11
RTR 4-9

S

serial interface 2-7
serialization delay 4-13
Session Manager 4-33
session target ras command 2-19
SGBP 4-29
sgbp member command 2-14
show modem command 2-43
show ppp queue command 4-25
show resource-pool resource command 4-30

show spe modem command 2-43

size command option 4-7

SLA 2-33

sliding windows applied to monitor number of incoming calls (figure) 4-8

SLIP 2-46

SLT 1-2

SNMP 2-3

enable community string parameter 4-35

enabling 4-35

enabling on gateway 2-37

traps 2-37

snmp-server command 2-37

SPE 2-43

spe command 2-43

spe command set 2-43

speech quality 4-9

spike 4-7

SS7

components for signaling 5-4

interconnect 5-4

resource group 4-31

resource groups 2-9

SS7 interconnect

references for voice and dial 2-11

stack groups 4-29

statistics 2-38

steps command option 4-7

syslog 2-36

T

T.38 fax relay 2-18, 2-50

and Microsoft NetMeeting 2-18, 2-21, 2-50, 3-3

T.38 mode request 2-21

T1

assigning controller 2-5

CAS FGB 2-4

CAS FGD 2-5

configuring controller 2-4

T3

configuring controller 2-5, 2-6

t38 keyword 2-21

tables

AAA Accounting Time Options and Their Definitions A-5

AAA Authentication Methods A-2

AAA Authorization Methods and Their Definitions A-3

AAA Methods and Their Definitions A-3, A-5

Bandwidth and Core Related Issues and Remedies 4-16

Call Threshold Trigger Options 4-6

Call Types and Rejection Criteria 4-3

Cisco Access Platforms and Recommended CEF and Cache Settings 2-42

Commonly Defined AAA Accounting Services A-4

Commonly Defined AAA Authentication Services A-1

Commonly Defined AAA Authorization Services A-3

Default SS7 Resource Group Mappings 4-32

ICPIF Values 4-9

Predefined SS7 Resource Groups 4-31

Resource Types for Defining Resource Groups (Port-Based and Non-Port-Based) 4-27

Traffic Classes and Types, with IP Precedence Numbers 4-11

Useful Cisco MIBs that Support the Cisco ASAP Solution 4-36

TACACS+

interface 2-3

tacacs-server command 4-25

tail-delay coverage 2-49

TDM

switching feature 2-22

Telemate 4-10

template-number 2-46

TFTP server

for IVR scripts 2-20

interface for 2-3, 2-6

time-slot interchange 2-22

timestamps 2-2, 2-6

time zone 2-2, 2-6

traffic classes and types, with IP precedence numbers (table) 4-11

transport input none command 2-13

treatment command option 4-5

triggers 4-5

tromboning 2-22

trunk cards 2-5

TSI 2-22

tunnel 2-15

two optimization models: simultaneous calls and calls per second (figure) 4-17

U

unified dial plan 2-17

universal port cards 5-2

URL xiii

useful Cisco MIBs that support the Cisco ASAP Solution (table) 4-36

user ID length 2-20

V

V.44 modem feature 2-47

V.92 modem feature 2-47

VAD 4-13

virtual access interface 2-45

virtual ISPs 4-26

virtual profile 2-45

virtual resource groups serving virtual ISPs (figure) 4-26

virtual template 4-21

virtual templates 2-15

voice ports

- and dial peers 2-18
- configuring 2-4

voice services

- enabling 2-17

voice service voip command 2-21, 2-22

VPDN

- configuring on gateway 2-15
- enabling on server 2-16
- group 2-33

vpdn enable command 2-16, 4-18, 4-21

vpdn group command 2-16

vpdn-group command 4-19, 4-21

VPN 2-15

vsa command option 2-25

VSAs

- and AAA billing 2-25
- defining for RADIUS 2-31

VSPT 5-6

W

Weblink Preferences xiv

WFQ 4-12

wildcards 2-23