Cisco ASAP Solution Overview and Planning Guide

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

Customer Order Number:
Text Part Number: OL-1395-01

CONTENTS

Preface vii

Document Version and Solution Release vii

Audience viii

Contents Overview viii

Document Organization viii

Related Documents ix

Viewing Online Documents in Your Browser ix

Terms and Acronyms x

Obtaining Documentation x

World Wide Web x

Documentation CD-ROM x

Ordering Documentation xi

Documentation Feedback xi

Obtaining Technical Assistance xi

Cisco.com xi

Technical Assistance Center xii

Cisco TAC Web Site xii

Cisco TAC Escalation Center xiii

CHAPTER 1 **Introduction** 1-1

Any Service, Any Port 1-1

The Cisco ASAP Solution 1-2

Layered Architecture 1-2

Elimination of Overlay Networks 1-4

Key Features of Unified Networks 1-4

Cisco IOS Features Enabled 1-5

Management 1-5

Resource Management 1-5

Element Management 1-6

Application Development 1-6

1-6

CHAPTER 2 **Solution Architecture and Services** 2-1

Basic Wholesale Voice and Dial Network Architectures 2-1

Basic Wholesale Voice Network Architecture 2-1

Basic Wholesale Dial Network Architecture 2-2

Merging Voice and Dial Services: Service Scenarios 2-3

Dial and Wireless Data 2-4

Network Diagram 2-4

Dial and Wireless Call Flow 2-5

PC to Phone 2-6

Network Diagram 2-6

PC-to-Phone Call Flow 2-7

Prepaid VoIP 2-8

Network Diagram 2-8

Prepaid VoIP Call Flow 2-9

Phone to Phone 2-10

Network Diagram 2-10

Phone-to-Phone Call Flow 2-11

Unified Communications 2-12

Network Diagram 2-12

Unified Communications Call Flow 2-13

TDM Switching 2-14

Support for DS0 Cross-Connections 2-15

Support for Call Types 2-15

T.38 Fax Service 2-16

CHAPTER 3 **Solution Components** 3-1

Universal Port DSPs and Universal Gateways 3-1

Major Components 3-2

Cisco Universal Gateways 3-3

Product Literature 3-4

Cisco Dial-Only Gateways 3-4

Product Literature 3-5

Cisco H.323 Gatekeepers and Directory Gatekeepers 3-5

Resource Management 3-6

Call Routing 3-6

Security 3-6

External GKTMP Applications 3-6

CDR Generation 3-6

Cisco Signaling Controllers 3-6

Cisco SS7 Signaling Link Termination Systems 3-7
Cisco L2TP Network Server 3-7
Cisco RPMS for Dial Services 3-8
Cisco Catalyst Switches 3-8
Additional Components (for Management and Shared Services) 3-8
Management Systems 3-10
Resource and Network Management Systems 3-10
Element Management Systems 3-11
RADIUS-Based Platforms 3-12
Cisco Access Registrar 3-12
RADIUS Proxy Server 3-13
Billing Systems 3-13
Unified Communications Application Server 3-14
TFTP Prompt Server 3-14
NTP Time Server 3-14

CHAPTER 4 **Designing a Solution** 4-1
Overview: Design Issues and Choices 4-1
H.323 Network Issues 4-1
Dial Plans and Number Normalization 4-2
Unified Dial Plans 4-2
Number Normalization 4-3
Dynamic Call-by-Call Handling 4-3
Call Control Scripts 4-3
Cisco TCL IVR 4-3
VXML 4-4
SS7 Interconnect 4-4
Network Design Guidelines 4-5
Guidelines for Individual Components 4-5
Guidelines for Gateways 4-5
Guidelines for Gatekeepers and Directory Gatekeepers 4-5
Guidelines for Cisco SC2200 Nodes 4-5
Solution Resilience 4-6
Traffic Engineering 4-6
Convergence and Migration Considerations 4-6
Contention 4-7
Additional Traffic Engineering Issues 4-9
Billing and Settlement 4-9

CHAPTER 5 **Solution Management** 5-1

Resource Management 5-1

Ensuring Quality of Service 5-2

Call Admission Control and RSVP 5-2

RSVP and RSVP-Based CAC 5-2

Low Latency Queuing 5-3

IP Precedence 5-3

Port Policy Management and Cisco RPMS 5-3

RADIUS PPM Server 5-4

Additional Network Management Tools 5-4

Cisco Info Center 5-4

Cisco Internet Performance Manager 5-5

Element Management Systems 5-5

Cisco Universal Gateway Manager 5-6

Cisco Voice Manager 5-6

Key Features in CVM 5-7

Cisco MGC Node Manager 5-8

Cisco Billing and Measurements Server 5-8

Cisco Voice Services Provisioning Tool 5-8

GLOSSARY

INDEX

Preface

The Cisco ASAP (Any Service, Any Port) Solution is a unified network architecture that delivers integrated data, voice, fax, and wireless data (V.110) services on a single platform, 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 preface presents the following major topics:

- Document Version and Solution Release
- Audience
- Contents Overview
- Document Organization
- Related Documents
- Terms and Acronyms
- Obtaining Documentation
- Obtaining Technical Assistance

Document Version and Solution Release

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

Audience

This document is part of a suite of documents for the following users:

- Candidate customers—who are able to take advantage of this solution and want to understand it
- Network operators/administrators—who have experience in telecommunications networks, protocols, and equipment, and a familiarity with data communications networks, protocols, and equipment
- Network designers—who have experience with telecommunications networks, protocols, and equipment, and experience with data communications networks, protocols, and equipment

For the other documents related to the Cisco ASAP Solution, see Related Documents, page ix.

Contents Overview

The *Cisco ASAP Solution Overview and Planning Guide* provides the following information:

- An introduction to the Cisco ASAP Solution, including the services it supports
- The solution's general architecture, network topologies, and components
- Deployment considerations, covering a variety of possible scenarios and issues that must be considered

This document does not provide detailed information on how to install and provision a given solution. Rather, it provides the background needed to understand the components, their interconnections, and key issues related to that solution. For the details of provisioning, refer to the *Cisco ASAP Solution Implementation Guide*.

Note Figures and tables are listed in the Index, under "figures" and "tables," respectively.

Document Organization

The major sections of this document are as follows:

Section	Title	Description
Preface	Preface	Provides an overview of this document and lists related resources.
Chapter 1	Introduction	Introduces the Cisco ASAP Solution, listing candidate customers, benefits and features, and services.
Chapter 2	Solution Architecture and Services	Discusses basic wholesale voice and wholesale dial network architectures, and presents a variety of service scenarios for converged services.
Chapter 3	Solution Components	Lists components needed to implement Cisco ASAP Solutions, including resource and element management applications.

Chapter 4	Designing a Solution	Discusses a variety of design issues and choices, including how to ensure quality of service (QoS) in a converged network.
Chapter 5	Solution Management	Discusses resource management features available in the Cisco IOS, as well as other network and element management systems.
Glossary	Glossary	Acronyms and terms used in this document.
Index	Index	Index

Related Documents

Refer to the following documents for detailed hardware and software installation and configuration information about the Cisco ASAP Solution:

- *Cisco ASAP Solution Implementation Guide*

  The above provides links to online references for the many components of the solution.
- *Cisco ASAP Solution Release Notes*

In addition, much related information is provided in the documents supporting the Cisco Wholesale Voice Solution, available at the following URL:

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

The *Cisco Wholesale Voice Solution Overview* provides background and design issues related to wholesale voice networks, and the *Cisco Wholesale Voice Solution Design and Implementation Guide* provides background and implementation scenarios related to provisioning, as well as links to additional useful documents. The above documents will be referred to later in this document with respect to issues that are common to the Cisco ASAP provisioning environment.

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.

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

Any Service, Any Port

Service providers must meet the demands of users who want access to Internet applications and services at any time, any place—on any device. To meet this need, Cisco introduces its ASAP architecture: Any Service, Any Port. The Cisco ASAP Solution is a unified architecture that allows service providers to deliver integrated data, voice, fax, and mobile wireless services at a profit. At the heart of the solution is the universal gateway, or UG—Cisco AS5350, Cisco AS5400, and Cisco AS5850 gateways that use a new universal port DSP (digital signal processor) that is capable of supporting voice and asynchronous data on the same DSP. These platforms also support SS7 signaling. (For more information, see Universal Port DSPs and Universal Gateways, page 3-1.)

Note The Cisco AS5300 and Cisco AS5800 do not currently use the new universal port DSP.

Reaching users through existing narrowband technologies is critical to earning revenue today, to sustain service providers through the long transition to broadband (both wireline and 3G wireless). Users want Internet services and applications wherever they go. The only solution to this problem is to deploy a single network that can handle different devices, meeting the needs of both end users and application developers alike. The Cisco ASAP Solution delivers an infrastructure that is both flexible and future-proof, preserving and maximizing capital investment.

The Cisco ASAP Solution benefits the following constituencies:

- End users, who want Internet services and applications at any time, on any device
- The wholesalers of both voice and data services

  Note Wholesaling refers to the management of voice or data ports by one carrier for use by service providers to deliver new services efficiently. The retail service provider, or "virtual service provider," simply leases these ports.

- Service providers, both wholesale and retail, who must deliver both voice and data services at a profit
- Application developers, who bring innovative Internet applications to market but currently cannot deliver multimedia applications with true carrier-class resiliency

This chapter presents the following major topics:

- The Cisco ASAP Solution
- Cisco IOS Features Enabled
- Management
- Application Development

The Cisco ASAP Solution

The Cisco ASAP Solution will not provide all possible features at its inception, but its layered architecture is designed to support their development.

Layered Architecture

Figure 1-1 illustrates the three basic components, or layers, that the Cisco ASAP Solution will provide as it evolves.

- At the front end, Cisco UGs terminate data, voice, fax, and wireless calls through open, programmable gateways (GWs).

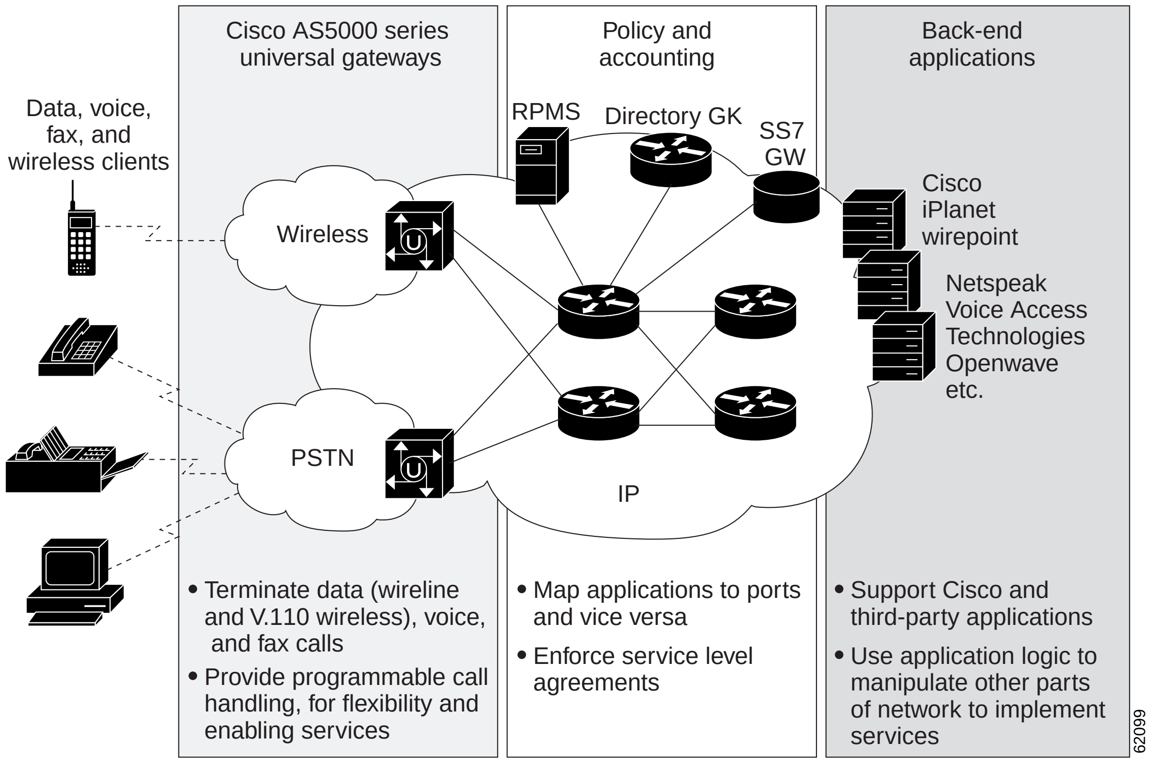
  This programmability is essential to service providers, who must rapidly adapt their infrastucture to new opportunities.

- At the back end, customers can use carrier-class services from a wide range of Cisco Ecosystem Partners, such as the following:
  - Openwave (http://www.openwave.com/)
  - Voice Access Technologies (http://www.voice-access.com/)
  - Digiquant (http://www.digiquant.com/)
  - MIND CTI (http://www.mindcti.com/)

  Again, the programmability of the UGs is essential to application developers, as it is the UG features that make services carrier class.

- In the middle, a layer of policy and accounting products map applications to ports and vice versa. In addition, these products authenticate user sessions, enforce service-level agreements (SLAs), and implement VoIP dial plans.

Figure 1-1 Cisco ASAP Solution Architecture



Elimination of Overlay Networks

Consider the traveler who needs to do the following:

- Use a modem to access and synchronize remote PC files to access a virtual assistant (such as that provided by Voice Access Technologies, Inc.
- Use a cell phone to use voice commands to access the virtual assistant (for example, to reach Yellow Pages)
- Make a wireless data call to a personal WAP (wireless access protocol) page (for example, to obtain directions)

In the not too distant past, our traveler would have needed three different networks:

- A wholesale dial network for the modem calls
- A wireless data network
- A managed VoIP network

However, using the above three networks entails considerable costs for the circuits, and circuit costs can be between 60 and 80 percent of revenue for the access service provider. When voice and data networks are overlaid, the circuit costs can be up to 100 percent higher than would be the cost for a single network. One reason multiple networks are inefficient is that voice and data networks achieve their maximum use at different times of day. A typical dialup network is busiest during the evening, whereas a voice network is busiest during the day.

To provide a cost-effective remedy to the above, the principle objective of the Cisco ASAP Solution is to unify the networks. Details of the architecture are presented in Chapter 2, "Solution Architecture and Services."

Key Features of Unified Networks

To unify networks, the Cisco ASAP Solution provides the following key features:

- Universal ports provide *any service on any port* of a universal GW *at any time*. Call types supported are modem, ISDN data, voice, fax, and wireless data (V.110).
- As all the above call types are implemented on a single *universal gateway*, capital costs are minimized and the complexity of preprovisioning GWs for different services is eliminated.
- A *unified dial plan* simplifies provisioning, by making it easy to map dialed numbers or trunks to different services.
- *Dynamic call-by-call handling*—offering any call type on any port—is the key software function that makes possible the use of universal DSP functionality, by mapping incoming calls to different service-implementation software running on the GW.
- *Enhanced call admission control* (CAC) ensures that a GW will never accept a call that it cannot complete, and will proactively inform network elements such as H.323 gatekeepers (GKs) when the GW is reaching capacity, to aid in intelligent voice/fax call-routing decisions.
- *Port policy management* ensures that, even though any call can be handled at any time, across the network as a whole, there is a consistent set of port-availability guarantees that will not be violated.
- Finally, because the UG is designed to support H.323 Session Initiation Protocol (SIP), as well as Media Gateway Control Protocol (MGCP), the service provider *is not limited* when it comes to network architecture and application protocol requirements—or those of prospective customers.

Note SIP and MGCP functionality are not available in initial releases of the Cisco ASAP Solution.

Cisco IOS Features Enabled

Beginning with Cisco IOS Release 12.2(2)XA, numerous features are made available for enhanced voice services, prepaid calling, wireless data, unified communications, wholesale dial, and wholesale VoIP. Table 1-1 lists the services enabled by the Cisco ASAP Solution.

Table 1-1 Features and Services Enabled by the Cisco ASAP Solution

• SS7 signaling	• Voice packetization G.711/G.729a/G.723.1 codecs, H.323
• Low-latency packet switching	• Out-of-band DTMF digit relay for value-added applications
• Wireless data (V.110) termination	• Hierarchical, scalable dial plans
• Built-in firewall and intrusion detection	• Foreign-language IVR support
• V.44 data compression	• Nonrepudiated accounting through OSP
• Remote access VPN service level agreements	• Support for SIP and MGCP[1] call control with third-party application integration
• Reverse Path Forwarding to block denial-of-service attacks	• RealAudio audio streaming for dynamic, on-demand content
• V.92 modem on hold per subscriber (per-call modem preconfiguration)	• Support for TCL and (later) VXML (VoiceXML)[2] scripting
• Dial PPP, V.92/V.90/V.42 RADIUS authentication	• T.38 real-time fax relay

1. SIP and MGCP are not supported in initial releases of the Cisco ASAP Solution.
2. VXML is not supported in initial releases of the Cisco ASAP Solution.

Management

There are two aspects to managing the Cisco ASAP Solution: managing resources, and managing network elements. These are discussed briefly in the following sections.

Resource Management

When you are running multiple applications in the same network, rather than one application per network, it is important to manage network resources. The Cisco ASAP Solution provides the ability to enforce both network-wide SLAs and per-gateway application-overload protection. A universal GW will never accept a call that violates a network-wide SLA, nor would it consume CPU resources that are in short supply at a given time. This resource management, coupled with hardware and software features, ensures that the availability of applications matches that of the network: “five nines.” In addition to providing any service on any port at any time, the Cisco ASAP Solution meets the following key objectives:

- Never connects calls to failed DSPs
- Takes failed trunks out of service as needed
- Takes failed DSPs out of service
- Handles application failure gracefully

For details, see Resource Management, page 5-1.

Caution A variety of IOS-based features are available now. However, in larger networks an application such as Cisco Resource Pool Managemer Server (RPMS) will be required to ensure SLAs. In initial releases of the Cisco ASAP Solution, Cisco RPMS is applicable to dial services only.

Element Management

To manage a Cisco ASAP network of any significant size, Cisco offers a variety of element management systems. Features include configuration, provisioning (including dial plans), fault management, network maps, performance monitoring, and acccounting, among others. For details, see Element Management Systems, page 5-5.

Application Development

To meet the needs of application developers who are creating innovative services, the Cisco ASAP Solution (following its initial releases) will use commonly available software development tools. Cisco ASAP will be able to map inbound calls to different applications, providing both Tcl (Tool Command Language, in particular Cisco TCL IVR) and VXML (Voice eXtensible Markup Language) scripting capabilities to enable the rapid development of distributed applications.

Solution Architecture and Services

This chapter introduces a variety of topologies that make up the architecture of the Cisco ASAP Solution. This provides a foundation for understanding the deployment of various services, and introduces a variety of issues that must be taken into consideration for each service or service mix.

This chapter presents the following major topics:

- Basic Wholesale Voice and Dial Network Architectures
- Merging Voice and Dial Services: Service Scenarios

Basic Wholesale Voice and Dial Network Architectures

The basic network architectures for wholesale voice (VoIP) and dial are not identical, assuming that each is specific to a single medium. As the utility of universal ports and universal gateways makes evident, such networks are becoming increasingly less practical for reasons of economics and management efficiency. Nevertheless, it is worthwhile to begin by discussing the differences.

Basic Wholesale Voice Network Architecture

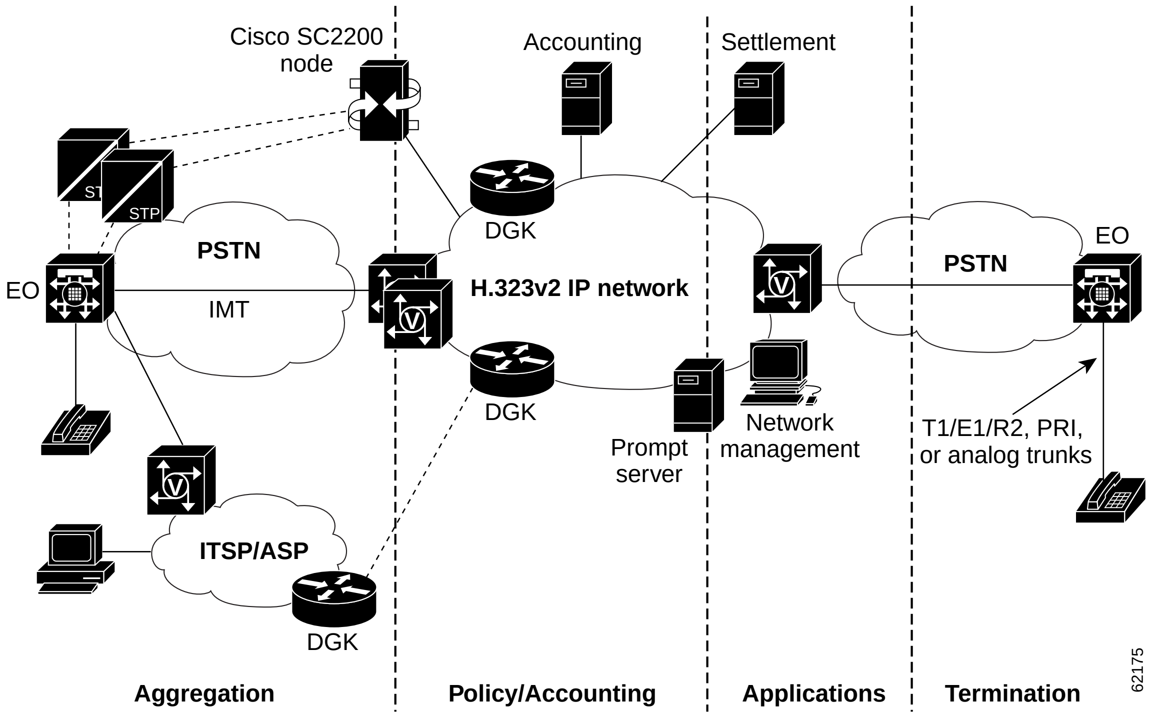
Figure 2-1 illustrates the basic architecture of a wholesale voice network. Note the following characteristics:

- PSTN end offices (EOs), supporting the subscriber at both aggregation and termination (ingress and egress) ends
- Voice-enabled gateways
- Support for SS7 signaling
- Accounting and settlement applications as needed, to support billing
- Prompt servers (such as IVR servers) as needed
- RADIUS and AAA servers (not shown) as needed, to support authenticaion and accounting
- Compliance with the H.323 protocol

Note Initial releases of the Cisco ASAP Solution do not provide support for SIP and MGCP.

Note For a detailed discussion of wholesale voice architectures and their requirements and features, see the documents provided for the Cisco Wholesale Voice Solution, at the following URL: http://www.cisco.com/univercd/cc/td/doc/product/access/sc/rel7/soln/wv_rel1/index.htm Documentation for the Cisco ASAP Solution will refer to these documents as needed.

Figure 2-1 Basic Wholesale Voice Network Architecture



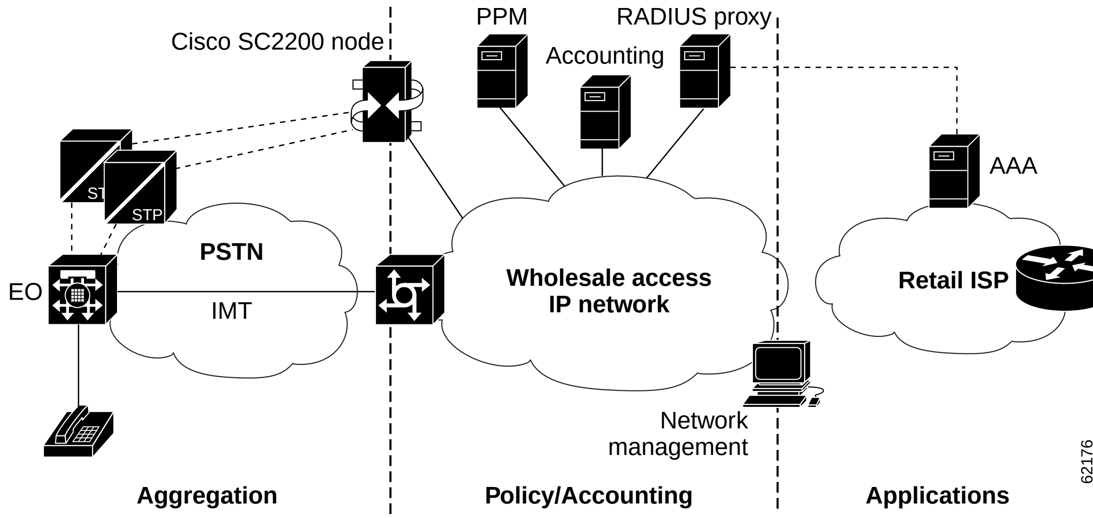
Basic Wholesale Dial Network Architecture

Figure 2-2 illustrates the basic architecture of a wholesale dial network. Note the following characteristics:

- A PSTN EO to support the subscriber at the aggregation end
- The absence of voice-enabled gateways
- RADIUS and AAA servers (not shown) as needed, to support authenticaion and accounting
- Port policy management (PPM) applications, to manage dial ports efficiently
- Support for SS7 signaling

Note In initial releases of the Cisco ASAP Solution, wholesale dial signaling is limited to SS7 functionality. However, SS7 signaling support is not always required.

Figure 2-2 Basic Wholesale Dial Network Architecture



Merging Voice and Dial Services: Service Scenarios

With the universal gateways (UGs), it is now possible to merge the voice and data worlds. An understanding of basic service scenarios, as well as their call flows, will make it easier to deploy a Cisco ASAP Solution successfully. Scenarios are presented below for the following services:

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

Note the following with respect to these services:

- The call flows are generalized to illustrate functional steps of interest in a given service. Protocol exchanges are not detailed.
- The details of access into the ITSP network are not shown, as access can take a variety of forms.
- It is assumed that GWs are configured to provide H.323 RAS messaging.
- SS7 infrastructure and signaling are not shown.
- H.323 call proxy servers are optional components that hide the identity of the originating endpoints. Their H.323 functionality is the same as that of an H.323-capable GW.

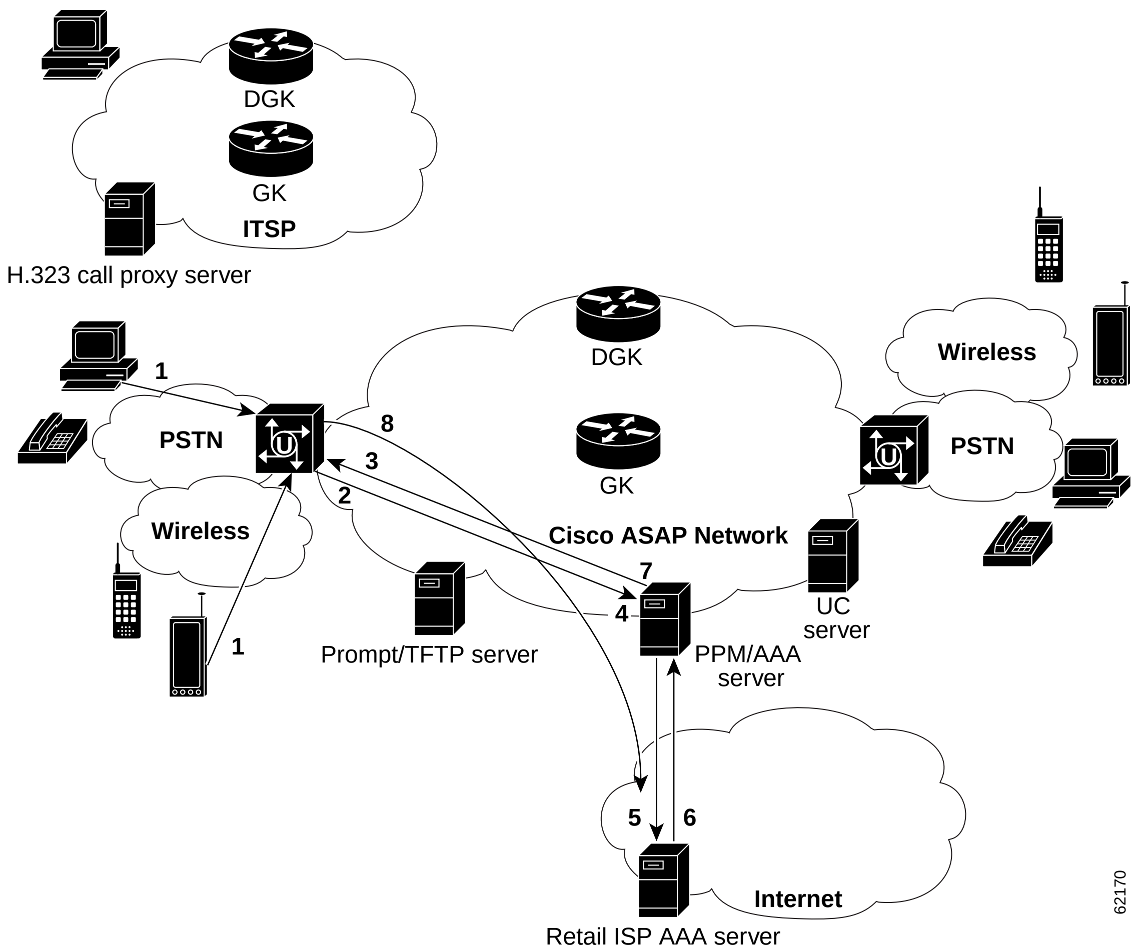
Dial and Wireless Data

Network Diagram

Figure 2-3 illustrates an example network and call flows for a dial and wireless data service. The call flow is described following the figure.

Note To simplify the illustration template in the figures that follow, "PPM/AAA server" can be either a PPM server (such as RPMS) or an AAA server. They are not the same entity. The call flows explicitly state the type of server that is addressed.

Figure 2-3 Dial and Wireless Data



Dial and Wireless Call Flow

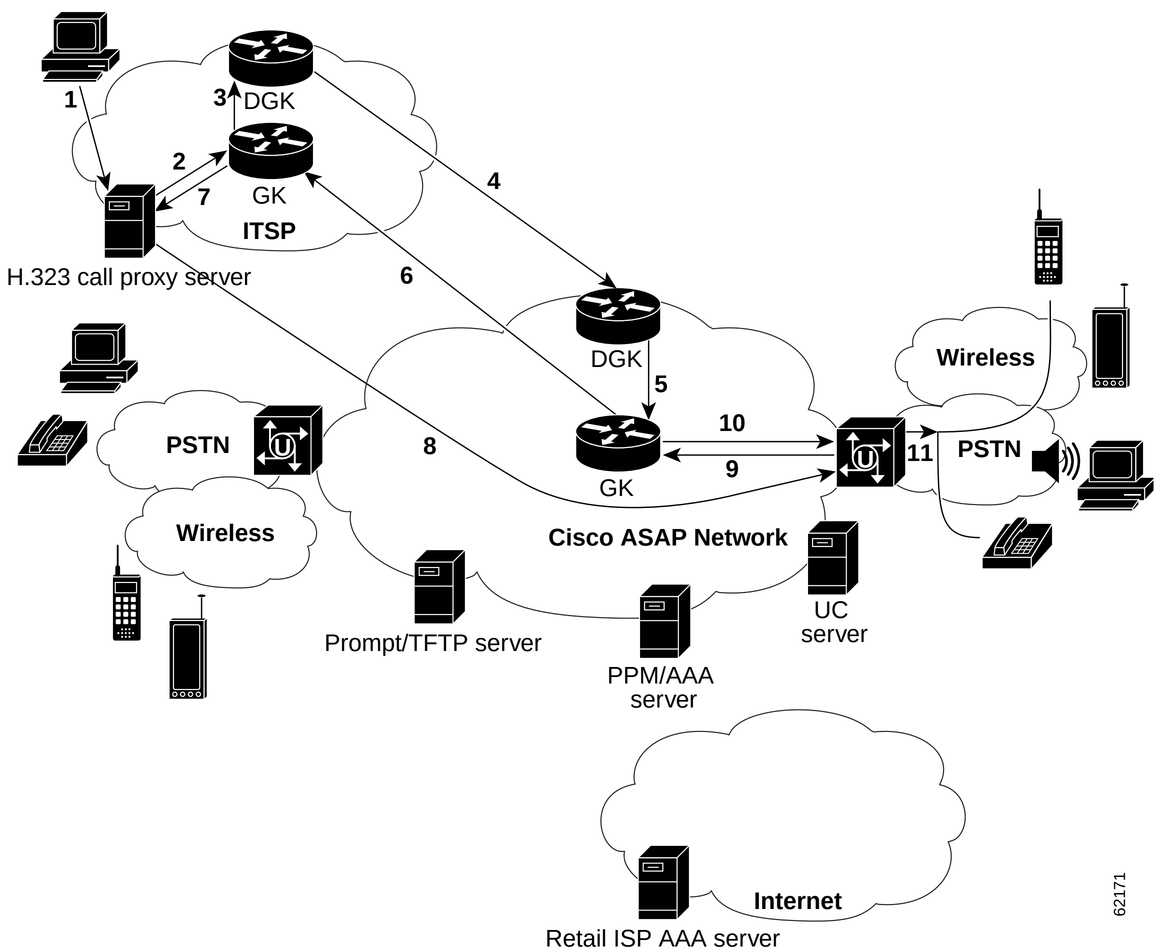
1. The subscriber's call arrives from the PSTN. This can be a traditional telephone call or wireless call, with the called number of a dial access service.
2. Before accepting the call, the GW sends a preauthentication request to the PPM server.
3. The PPM server checks the port policy for the retail ISP and returns information to the GW as to whether to accept or reject the call. The following step assumes the call is accepted on the PPM server.
4. The GW accepts the call and authenticates the user by sending an authentication request to the AAA server.
5. If the AAA server is performing a RADIUS proxy role, it will forward the authentication request to the retail ISP's AAA server.
6. The retail ISP's AAA server either accepts or denies the user, and returns this status to the RADIUS AAA proxy server. The following step assumes the call is accepted by the retail ISP's AAA server.
7. The RADIUS AAA server forwards the acceptance status to the originating GW.
8. The user's call enters the Internet.

PC to Phone

Network Diagram

Figure 2-4 illustrates an example network and call flows for a PC to phone service. The call flow is described following the figure.

Figure 2-4 PC to Phone



PC-to-Phone Call Flow

1. The subscriber at a PC with VoIP software "dials," sends an admission request to an H.323-based call proxy server, which functions as the OGW.

Note For an illustration of H.323 RAS messaging and further reference, refer to Chapter 2, "Provisioning the Gatekeeper Core," of the *Cisco Wholesale Voice 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 user is assumed to be "registered" on the call proxy server, which authenticates the subscriber.

2. Following a successful challenge, the call proxy server queries the local GK as to where to send the call.

   In this example, the call terminates in another zone.

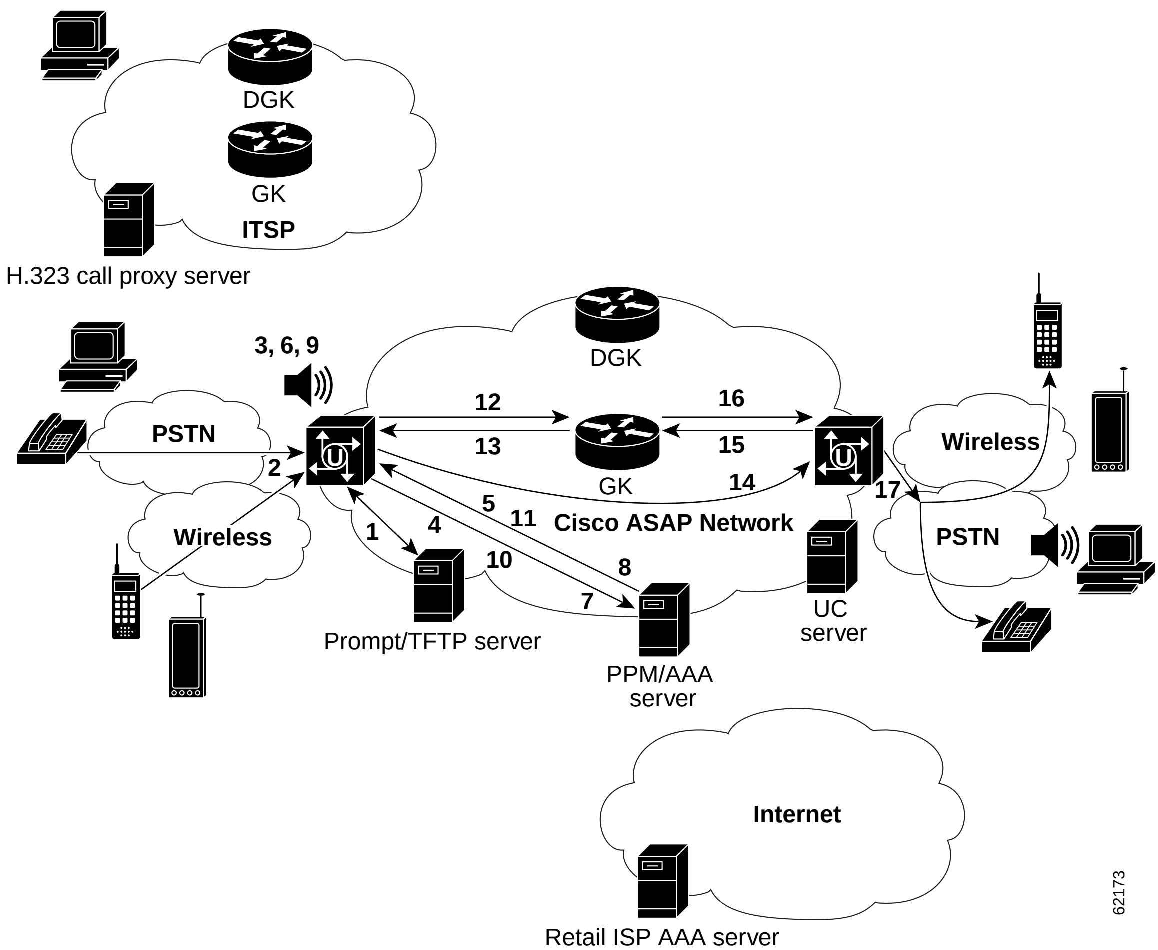
3. The zone (originating) GK forwards the location request to the ITSP DGK.
4. The ITSP DGK queries the DGK in the Cisco ASAP network.
5. The Cisco ASAP DGK sends a location request to its zone (terminating) GK to confirm that the requested E.164 address can be serviced.
6. If so, the terminating GK confirms this to the originating GK.
7. Following the successful confirmation, the originating GK sends a confirmation to the OGW.
8. The call is set up between the call proxy server and the TGW.
9. The TGW sends a request for admission to the terminating GK.
10. The terminating GK sends confirmation that the address can be serviced.
11. The call proceeds to a wireline or wireless network.

Prepaid VoIP

Network Diagram

Figure 2-5 illustrates an example network and call flows for a RADIUS-based prepaid phone service. Ingress trunks are SS7, and egress trunks are SS7, CAS, or PRI. This is similar to Dial and Wireless Data, page 2-4, except that (1) RADIUS is used exclusively, (2) there are no interconnections between different SPs, and (3) the RAS messaging is illustrated. In addition, no DGK-DGK transactions are required as in PC to Phone, page 2-6, as this example assumes a single zone. The call flow is described following the figure.

Figure 2-5 Prepaid VoIP



Note RADIUS-based prepaid calling, including some third-party applications used to realize it, is discussed extensively 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

Prepaid VoIP Call Flow

1. Prompt scripts previously loaded to prompt/TFTP server are downloaded to originating (ingress) GW.

   Such a server is ideal for holding large and multiple audio files, which can be downloaded dynamically as required.
2. The subscriber's call arrives from the PSTN. This can be a traditional telephone call, with the called number of a prepaid service.

   On the OGW, the called number matches a dial peer with a call to an application of type, for example, "debit-card."
3. The appropriate IVR audio file is played. This welcomes the user and prompts the user for an account number.
4. The user enters an account number and the OGW collects the number (as DTMF tones) and passes it to a AAA server in the Cisco ASAP network for verification.
5. If the number matches the user's account number in the AAA database, the AAA server so notifies the OGW.
6. The appropriate IVR audio file on the OGW prompts the user to enter a PIN.
7. The OGW passes the PIN information to an AAA server for verification.
8. On a successful PIN match, the AAA server forwards confirmation to the OGW.
9. The appropriate audio file on the OGW prompts the user for a number to dial.
10. The OGW passes the called number to the AAA server.
11. The AAA server confirms or denies admission.

Note Only on a confirmation does the following take place.

12. The OGW forwards the request for admission to the Cisco ASAP DGK.
13. The Cisco ASAP DGK responds affirmatively to the OGW that the TGW can handle the call.
14. The call is set up between the OGW and the TGW.
15. The TGW sends a request for admission to the GK.
16. The GK sends confirmation to the TGW.
17. The call proceeds to wireline or wireless networks.

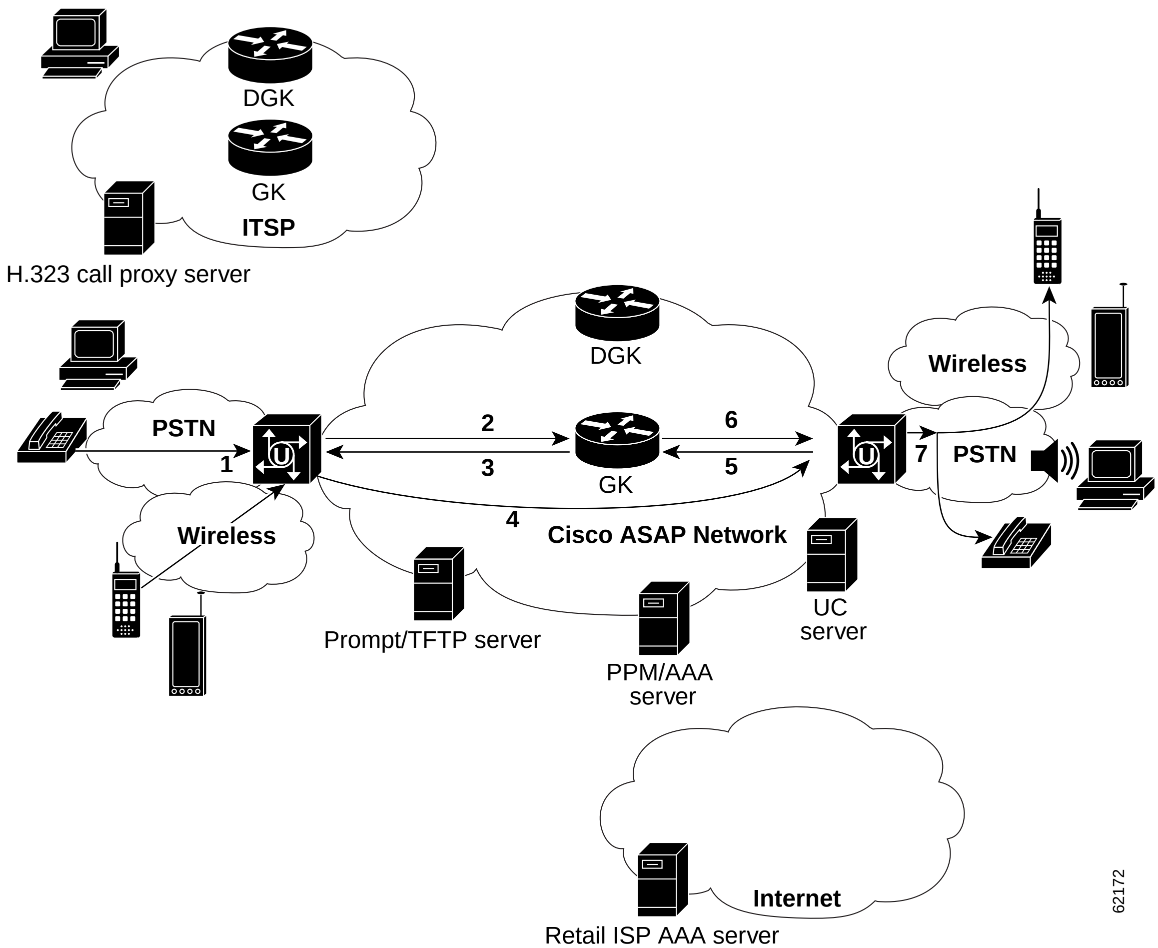
Phone to Phone

Network Diagram

Figure 2-6 illustrates an example network and call flows for a simple phone-to-phone service. No transactions other than RAS are involved. The call flow is described following the figure.

Note Long-Distance Toll Bypass, page 2-11, illustrates an application of phone-to-phone service for bulk use by ISPs; the implementation is the same.

Figure 2-6 Phone to Phone



Phone-to-Phone Call Flow

1. The subscriber's call arrives from the wireline or wireless PSTN.

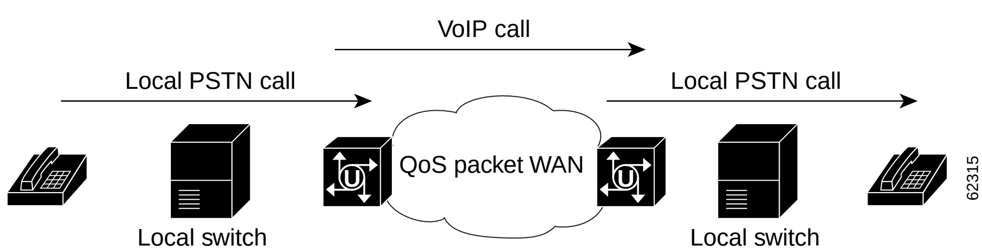
   No interactive prompts are involved.
2. The OGW forwards a request for admission to the Cisco ASAP GK.
3. The Cisco ASAP GK sends confirmation to the OGW.
4. The call is set up between the OGW and the TGW.
5. The TGW sends a request for admission to the Cisco ASAP GK.
6. The Cisco ASAP GK sends confirmation to the TGW.
7. The call proceeds to wireline or wireless networks.

Long-Distance Toll Bypass

Long-distance toll bypass is an application of phone-to-phone service that is well-suited to the bulk call-routing needs of certain ISPs. By leveraging their existing data infrastructure and subscriber bases, ISPs can deliver carrier-class long-distance voice services over low-cost IP networks. With universal GWs as VoIP GWs, the Cisco ASAP Solution allows ISPs to carry voice traffic over packet networks, offering carrier-class domestic and international phone calls. Subscribers make long-distance calls from a regular telephone at home or office, or from other locations by entering an account number or password. No server lookup or IVR is needed. Calls are forwarded from the PSTN through the ingress UG to the egress UG, simply on the basis of the dial peer configuration, in a manner similar to TDM switching (see TDM Switching, page 2-14). Ingress trunks are SS7, and egress trunks are SS7, CAS, or PRI. Figure 2-7 illustrates the toll-bypass feature.

Note This feature is also supported on Cisco VoIP-enabled GWs.

Figure 2-7 Long-Distance Toll Bypass



Unified Communications

Unified communications services are provided by third parties, and include such solutions as voice mail over IP, fax store and forward, single-number reach, and so on. In addition, refer to Cisco's Internet Communications Software at the following URL:

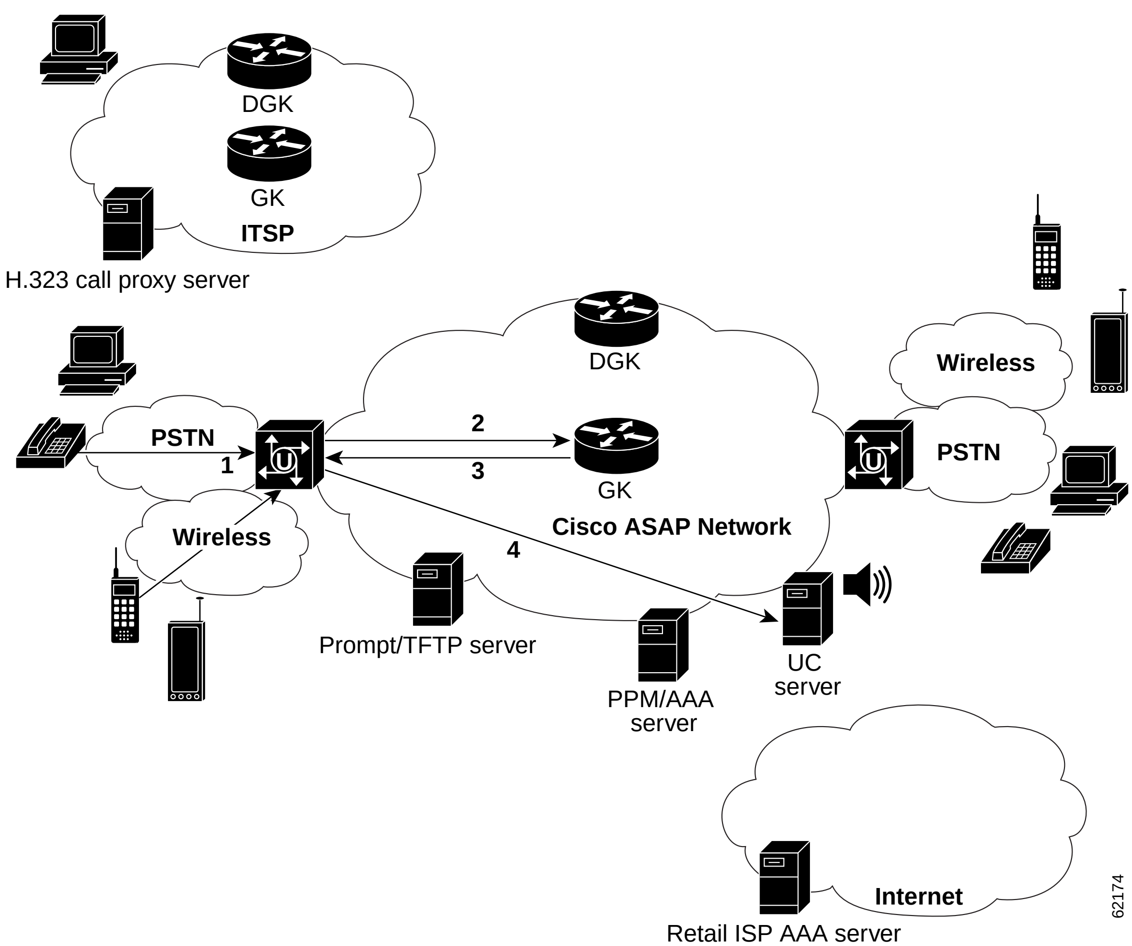
http://www.cisco.com/warp/public/180/

Network Diagram

Figure 2-8 illustrates an example network and call flows for a unified communications (UC) service. This view is quite simplified. Depending on the size of the network, UC servers can require substantial capabilities (they perform considerably more signaling and functionality than is shown here) and are often clustered in server farms. The call flow is described following the figure.

Note Initial releases of the Cisco ASAP Solution do not support T.37 (store-and-forward fax through e-mail, using SMTP and MIME).

Figure 2-8 Unified Communications



Unified Communications Call Flow

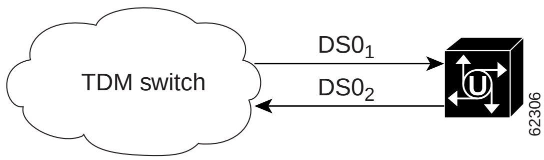
1. The subscriber's call arrives from the wireline or wireless PSTN.
2. The OGW sends a request for admission to the Cisco ASAP GK.
3. The Cisco ASAP GK sends confirmation to the OGW.
4. The call proceeds to the UC server, to be handled in a variety of possible ways.

Tip For detailed technical discussion of unified messaging and its capabilities, refer to Unified Messaging at the following URL:
http://www.cisco.com/univercd/cc/td/doc/cisintwk/intsolns/voipsol/um_isd.htm

TDM Switching

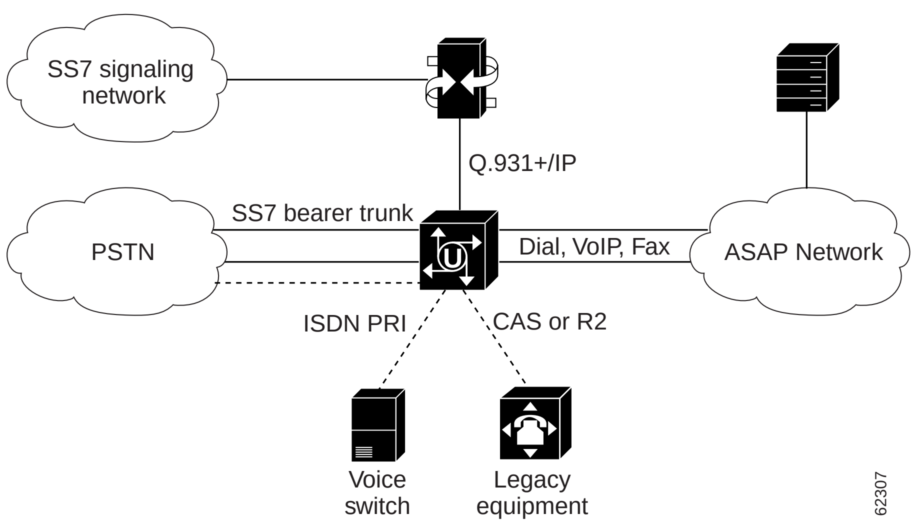
TDM switching is the ability of Cisco UGs to switch information directly between two DS0 circuits without affecting the data. Figure 2-9 illustrates this feature. The two calls, one incoming and one outgoing, are connected through a time slot interchange (TSI) function in the DS1/DS3 trunk card.

Figure 2-9 TDM Switching



This feature allows legacy systems to be maintained while new services are added. As demonstrated in Figure 2-10, the SP can migrate gracefully to Cisco ASAP technology while redirecting calls (dotted lines) to legacy equipment or PSTN switches as needed. With support for PRI and CAS, legacy systems can continue to be used.

Figure 2-10 Migration from Legacy and PSTN Services



The following additional benefits can also be realized:

- Cisco UGs are well-suited to customers requiring PRI grooming in conjunction with VoIP, dial, and fax services.
- Interconnect costs are reduced. IMT (SS7) trunks are 40 to 70% cheaper than PRI trunks.

Note Initial releases of the Cisco ASAP Solution do not support SS7-to-SS7 switching with ISUP transparency.

- External test equipment is supported. TDM switching can be used to connect test-tone generating devices. Type 105 test tones in the Cisco UGs can be provided by connecting to external text equipment through TDM cross-connections.

Support for DS0 Cross-Connections

TDM switching is supported on T1, E1, and DS3 interface cards. In Cisco UGs, both trunk and DSP cards provide onboard TSI functionality. DS0 channels used in TDM-switched calls can come from the same T1/E1 interface or different T1/E1 interfaces in the GW. Once two DS0s are cross-connected, the TSI circuitry is responsible for transmitting and receiving PCM data to and from the two DS0s. The circuitry also makes it possible to include any type of bearer data. Any ingress (received) DS0 on any DS1 or DS3 can be switched to an egress (transmit) DS0 on the same or a different DS1 or DS3.

Special Issues

Note the following special issues with respect to the DSP resources used in TDM switching:

- *Switching between SS7-CAS or PRI-CAS*

  When a CAS trunk is involved in TDM switching (on any Cisco GW), the DSP resource is required to set up the connection. This resource stays in the call path once the call is established. This is required to monitor the inband signaling (A, B, C, and D bits), so that the call can drop normally. With non-CAS calls, no DSP resources are used after the call connection is established.

- *CAS-to-CAS Calls*

  If two CAS calls are involved in the TDM switching session, then each leg of the call uses one DSP resource. Once the call is established, both resources stay in the call path to monitor the inband signaling (A, B, C, and D bits), so that the call can drop normally.

- *Interactive Voice Response*

  VoIP calls using interactive voice response (IVR) in any portion of the call legs will also use DSP resources. When an incoming call uses IVR functionality, the DSP resource is not released until the call is released.

Support for Call Types

Table 2-1 shows the types of calls supported by TDM switching in the Cisco ASAP Solution.

Table 2-1 Types of Calls Supported by TDM Switching

Origination/Termination	Comments
SS7/PRI	Incoming calls originate on IMTs (SS7 trunks), terminate on ISDN PRI trunks. Incoming calls originate on ISDN PRI trunks, terminate on IMTs. Both network-side and user-side PRI interfaces are supported. Both E1 and T1 are supported.
SS7/SS7	Incoming calls originate and terminate on IMTs, using the same ISUP variant.

Note In initial releases of the Cisco ASAP Solution, SS7-to-SS7 TDM switching with ISUP transparency is not supported. In addition, for outgoing calls, the GW cannot select a specific group of IMTs, which may be connected to a specific switch, as the GW does not currently support multiple trunk groups.

Table 2-2 shows the support for ISUP in VoIP calls originating from the PSTN.

Table 2-2 Types of ISUP VoIP Calls Supported by TDM Switching

ISUP Interface	Comments
ISUP to ISUP	Voice calls originate in the PSTN with SS7 signaling, traverse the H.323 VoIP network, and terminate in the PSTN on IMTs.
ISUP to CAS	Voice calls originate in the PSTN on IMTs, traverse the H.323 VoIP network, and terminate in the PSTN on CAS trunks.
ISUP to PRI	Voice calls originate or terminate in the PSTN with SS7 signaling, traverse the VoIP network, and terminate or originate in the PSTN on PRI trunks.

T.38 Fax Service

The Cisco ASAP Solution supports Cisco T.38 Real-Time and Never-Busy Fax Service. For details, refer to Fax Services at the following URL:

http://www.cisco.com/univercd/cc/td/doc/cisintwk/intsolns/voipsol/fax_isd.htm

Solution Components

To support the various topologies and applications of the Cisco ASAP Solution, both Cisco and third-party components are required. Some components are required in all topologies. Other components, although optional, are mandatory for certain solutions (such as those requiring SS7 signaling). This chapter lists and discusses the actual components, both Cisco's and those of third parties, that can be used to implement a Cisco ASAP Solution.

This chapter presents the following major topics:

- Universal Port DSPs and Universal Gateways
- Major Components
- Additional Components (for Management and Shared Services)

Universal Port DSPs and Universal Gateways

At the heart of the solution is the universal port DSP, which defines what are known as universal gateways (UGs). This digital signal processor supports both data and full-featured voice processing. In addition, DSP firmware is assigned dynamically, so that no static preprovisioning of the DSPs is required. This greatly reduces maintenance overhead, particularly in networks with large numbers of subscribers. Table 3-1 lists the voice and data features supported by the universal DSP.

Table 3-1 Voice and Data Features of the Universal DSP

Voice Features	Data Features
Support for industry-leading CODECs: G.711, G.729a, G.723.1	Support for the following formats: V.92, V.44, V.90, V.110, V.120, PIAFS
Support for T.38 fax relay	
G.168-compliant echo cancellation, programmable up to 128 msec	
Programmable frame size	
Generation and detection of DTMF and MF tones	

In addition, all members of the UG product line have the following in common:

- The Cisco IOS software codebase
- The DSP subsystem
- SS7 capabilities
- Trunking hardware
- Wireless data functions

With data and voice now accommodated dynamically, unified dial plans can be used to differentiate services on a call-by-call basis. (For a discussion of dial plans, see Dial Plans and Number Normalization, page 4-2.)

Major Components

Table 3-2 summarizes the major components, all of which are Cisco components. Required components are listed first, followed by optional components.

Note Refer to the most current *Cisco ASAP Solution Release Notes* for the latest information regarding IOS versions, other application software, and the platforms they run on.

Table 3-2 Major Components of the Cisco ASAP Solution

Component	Description
Cisco Universal Gateways	*Required*. Use universal DSP to support both voice and data. Support small- to large-scale interconnects with wholesaler's TDM-based customers. Platforms include the Cisco AS5350 and Cisco AS5400.
Cisco Dial-Only Gateways	*Optional*. Platforms include the Cisco AS5300, Cisco AS5800, and Cisco AS5850[1].
Cisco H.323 Gatekeepers and Directory Gatekeepers	*Required to support VoIP with RAS messaging*. Allow voice network to be scaled to large sizes. Platforms include the Cisco 3660 and Cisco 7200.
Cisco Signaling Controllers	*Optional*. However, these components are *required* in SS7 interconnect solutions. The supported platform is the Cisco SC2200 running Cisco SS7 Interconnect for Voice Gateways.
Cisco SS7 Signaling Link Termination Systems	*Optional*. However, these components are *required* in SS7 interconnect solutions. The platform is currently the Cisco 2611, although other platforms may be available in later releases of the Cisco ASAP Solution.

Table 3-2 Major Components of the Cisco ASAP Solution (continued)

Component	Description
Cisco L2TP Network Server	*Optional*. Any L2F/L2TP-compliant tunnel endpoint (home gateway). Provides large-scale L2TP tunnel aggregation. The Cisco 7200 VXR, among other platforms, can provide this service.
Cisco RPMS for Dial Services	*Optional*. Release 1.1 recommended for dial services. Enables port policy management (PPM) across multiple GWs.
Cisco Catalyst Switches	*Optional*. Both Cisco Catalyst 5000 and 6000 series switches are used. Cisco recommends Cisco Catalyst 6000 series switches for best VoIP QoS.

1. Initial releases of the Cisco ASAP Solution do not support voice services on the Cisco AS5850.

The following sections discuss the components in the table.

Cisco Universal Gateways

The Cisco ASAP Solution requires a range of small-, medium-, and large-scale PSTN interconnects with the wholesaler's TDM-based customers (typically IXCs, PTTs, or other wholesalers), depending on anticipated call volumes. Platforms include the Cisco AS5350 and the Cisco AS5400, along with various supporting network modules.

Note In the context of dial services, the above platforms are most frequently referred to as network access servers, or NASs. In the context of H.323 voice services, these platforms are most frequently referred to as gateways, or GWs. H.323 is currently the only signaling protocol used by the Cisco ASAP Solution for VoIP services. In initial releases of the Cisco ASAP Solution, SIP- and MGCP-based services are not supported.

For the interface modules and signaling types supported by the Cisco UGs, see Table 3-3.

Table 3-3 Cisco Universal Gateways, Interface Modules, and Supported Signaling Types

Platform	Interface Modules	Universal Port Capacity
Cisco AS5350	T1, E1, T3[1]	T1/E1: 8 T3[1] Ports: 216 universal
Cisco AS5400	T1, E1, T3, CT3	T1/E1: 16 PRI (voice) T3[2] (data) Ports: 384 universal, 648 data

1. Available to reduce provisioning costs, although only 8 T1s can be enabled.
2. T1 or T3 configuration.

Caution The Cisco AS5400 does not support both T1 and E1 dial feature cards (DFCs) in the chassis at the same time.

Note Currently, the Cisco 2500, Cisco 2600, and Cisco 3600 series routers are not supported by the Cisco ASAP Solution.

Product Literature

For product literature for the universal gateways, including data sheets, refer to the following URLs:

- Cisco AS5350 Universal Gateway

  http://www.cisco.com/warp/public/cc/pd/as/as5300/prodlit/index.shtml
- Cisco AS5400 Universal Gateway

  http://www.cisco.com/warp/public/cc/pd/as/as5400/prodlit/index.shtml
- Cisco AS5850 Universal Gateway

  http://www.cisco.com/warp/public/cc/pd/as/5850/prodlit/index.shtml

Cisco Dial-Only Gateways

In addition to universal gateways, the Cisco ASAP Solution supports the Cisco AS5300, Cisco AS5800, and Cisco AS5850 for dial-only service.

For the modules and signaling types supported by the Cisco dial GWs, see Table 3-4.

Table 3-4 Cisco Dial-Only Gateways, Interface Modules, and Supported Signaling Types

Platform	Interface Modules	Universal Port Capacity
Cisco AS5300	T1, E1	T1/E1: 8 Ports: 240 dial, 120 voice
Cisco AS5800	T1, E1, T3	T1/E1: 16 PRI (voice) T3[1] (data): 3 Ports: 72 T1/E1, 2047 dial, 1344 voice
Cisco AS5850[2]	E1, T3	E1: 86 T3: 4 Ports: 2688 dial

1. T1 or T3 configuration.
2. Voice (sub-T3) is not supported.

Product Literature

For product literature for the dial-only gateways, including data sheets, refer to the following URLs:

- Cisco AS5300 Universal Access Server
  http://www.cisco.com/warp/public/cc/pd/as/as5300/prodlit/index.shtml
- Cisco AS5800 Access Server
  http://www.cisco.com/warp/public/cc/pd/as/as5800/prodlit/index.shtml
- Cisco AS5850 Universal Gateway
  http://www.cisco.com/warp/public/cc/pd/as/5850/prodlit/index.shtml

Cisco H.323 Gatekeepers and Directory Gatekeepers

Cisco H.323 GKs and DGKs constitute the gatekeeper core. GKs are mandatory network elements used to scale a wholesale network to large sizes. Directory GKs (DGKs) further supplement network scalability and are mandatory if GK-based carrier interconnect is desired. The Cisco GKs and DGKs supported by the Cisco ASAP Solution are essentially IOS software images loaded onto a dedicated Cisco 3660 or Cisco 7200 series platform. Signaling among H.323 components is through RAS (Registration, Admission, and Status Protocol).

Note The Cisco ASAP Solution does not support integrated GKs and GWs.

Cisco GKs perform the following tasks.

Resource Management

Cisco GKs determine the health of H.323 gateways by monitoring registration and unregistration (RRQ/URQ) messages and resource availability indicators (RAIs).

Call Routing

Cisco GKs provide call routing based on destination E.164 addresses. They may use their knowledge of local GW health levels to make routing decisions in order to increase the network availability of the GWs. Cisco GKs may also route calls between remote GKs within the same administrative domain by means of inter-GK LRQ (location request) RAS messages. Similarly, Cisco DGKs may also route calls to other carrier administrative domains by means of LRQ RAS messages.

Security

Cisco GKs, in conjunction with an external server (such as RADIUS), may be used for secure call admission in intradomain call scenarios (calls within the same service provider's domain). Cisco GKs also have limited applications in implementing interdomain security functions for calls sent between carriers by means of IP interconnect.

External GKTMP Applications

Cisco GKs may act as a control point from which an application server can affect call routing, number translation, call admission/blocking, and the like. These application servers interface with a Cisco GK or DGK by means of GKTMP (Gatekeeper Transaction Message Protocol).

Note The Cisco ASAP Solution does not specify any particular GKTMP application, but does not exclude any from being used.

CDR Generation

Cisco GKs have limited abilities to generate CDR reports for calls either in addition to or instead of generating them from the GW. This is an option if the wholesaler either does not own the GWs at a point of presence (POP), or simply wants to reduce the amount of messaging overhead associated with AAA in its smaller POPs. However, billing in this manner has limitations.

Cisco Signaling Controllers

These optional components are used in SS7 interconnect solutions. The supported platform is the Cisco SC2200 running Cisco SS7 Interconnect for Voice Gateways.

Note Refer to *Cisco ASAP Solution Release Notes* for the software versions that are required.

Cisco SS7 Signaling Link Termination Systems

These optional components are used in SS7 interconnect solutions (where they are required). Signaling link termination (SLT) systems are Cisco 2611 platforms that are capable of terminating MTP1 and MTP2 SS7 layers and backhauling MTP3 and higher SS7 layers to the Cisco SC2200 in an SS7 interconnect application.

Cisco SLTs can be either colocated or located remotely with respect to the Cisco SC2200 hardware platform. However, with remote location, there are latency and loss requirements that must be met.

Caution Contact your Cisco account representative for a discussion of the issues involved in locating a Cisco SLT remotely from a Cisco SC2200 platform.

Cisco L2TP Network Server

L2TP (Layer 2 Tunneling Protocol) is the emerging IETF standard for Layer 2 tunneling (or building access Virtual Private Networks, or VPNs); it is compatible with the earlier L2F protocol. An extension of PPP, L2TP handles the server side of the L2TP protocol. The L2TP network server (LNS) is the initiator of outgoing calls and the receiver of incoming calls.

Note For a brief description of L2TP and the role of the LNS, refer to Fact Sheet: Layer 2 Tunneling Protocol—A Feature in Cisco IOS Software at the following URL:
http://www.cisco.com/warp/public/cc/pd/iosw/prodlit/l2tun_ds.htm

Traditional dial-up networking services support only registered IP addresses, which limits the types of applications that can be implemented over VPNs. L2TP supports multiple protocols and both unregistered and privately administered IP addresses over the Internet.

An LNS, also known as a home gateway, operates on any platform capable of PPP termination. The Cisco ASAP Solution can use, for example, the Cisco 7200 VXR broadband services aggregators as an LNS, to terminate VPDN tunnels for dial services. The total number of tunnels determines the maximum number of sessions a single LNS can handle. A single Cisco 7200 VXR can accommodate 1000 tunnels, and up to 8 sessions within each tunnel, for a total of 8000 sessions. User information can be stored locally, but it is most frequently stored on an AAA server.

Cisco RPMS provides support for L2F/L2TP tunnel definition (VPDN access) and tunnel policy management for dial calls. See Cisco RPMS for Dial Services, page 3-8, and Cisco Resource Pool Manager Server, page 3-10.

Note The Cisco 7200 VXR is not required. Cisco AS5400 and Cisco 6400 platforms can also perform this function, as can third-party equipment.

For more information about the platform, refer to Cisco 7200 VXR at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/core/7200vx/index.htm

For more information about LNS and VPDN, 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

Refer also to L2TP Tunnel Switching at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121limit/121dc/121dc1/l2switch.htm

Cisco RPMS for Dial Services

To enable port policy management for dial services across multiple GWs, a Cisco RPMS may be required. This makes it possible to model customers, services, and regions according to DNIS, trunk, or GW.

For more information, see the following:

- Cisco Resource Pool Manager Server, page 3-10
- Port Policy Management and Cisco RPMS, page 5-3

Cisco Catalyst Switches

Cisco Catalyst switches running ISL trunking are optional but useful adjuncts to traffic management in the Cisco ASAP Solution. Both Cisco Catalyst 5000 and 6000 series are used. For more information, refer to Multilayer LAN Switches at the following URL:

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

Note Cisco recommends Cisco Catalyst 6000 series switches for best VoIP QoS.

Additional Components (for Management and Shared Services)

This section discusses the additional components, both Cisco's and those of third parties, that support shared services such as management and billing. Table 3-5 on page 3-9 summarizes these components, which are provided by third parties.

Table 3-5 Additional Components of the Cisco ASAP Solution

Component	Description
Management Systems	*Traffic and Network Management Systems* • Cisco Resource Pool Management (RPM) and Cisco Resource Pool Management Server (RPMS) provide aggregation and allocation of dial resources. • Cisco Info Center (CIC) supports fault management and event correlation. • Cisco Internet Performance Manager (IPM) monitors performance of SP networks, with emphasis on QoS for VoIP. *Element Management Systems* • Cisco Universal Gateway Manager (UGM) helps manage access GWs. • Cisco Voice Manager (CVM) supports VoIP configuration and dial plan provisioning. • Cisco MGC Node Manager (CMNM) provides a CORBA-based fault, configuration, accounting, and performance management system (FCAPS). • Cisco Voice Services Provisioning Tool (VSPT) provides configuration and provisioning.
RADIUS-Based Platforms	• Cisco Access Registrar (an access policy server and proxy server for multiple services) • AAA database servers • RADIUS-based prepaid calling servers • RADIUS proxy servers
Billing Systems	Partition billing among SPs for voice and other services (typically are AAA/RADIUS based). The Cisco Billing and Measurements Server (BAMS) can also be used.
Unified Communications Application Server	Supports unified messaging.
TFTP Prompt Server	Maintains prompt database for GWs using interactive voice response.
NTP Time Server	Provides accurate timing across the network. Essential for billing and proper troubleshooting.

Management Systems

Resource and Network Management Systems

The Cisco ASAP Solution can take advantage of a variety of resource management systems, such as those that deal with port policy.

Network management systems (NMSs) are also optional components that are used for network monitoring, fault management, trap correlation, and reporting. Any NMS can extract this information from wholesale components through a variety of methods, such as SNMP, syslog, and AAA.

The following resource and network management systems can be used in the Cisco ASAP Solution:

- Cisco Resource Pool Manager Server
- Cisco Universal Gateway Manager
- Cisco Voice Manager
- Cisco Info Center
- Cisco Internet Performance Manager

These components are discussed in detail in the sections that follow.

Cisco Resource Pool Manager Server

Eliminating contention by controlling access to ports is critical to dial services. (Support is not yet provided for eliminating contention on voice ports.) The Cisco RPM (resource pool management) feature enables wholesalers to aggregate their dial resources across multipleUGs, and allocate subsets of these resources to retail ISPs. Cisco RPM allows providers to count, control, and manage dial resources, while also accounting for shared resources when different SLAs are implemented. RPM can be achieved by using the RPM component of the resource pooling solution on the UG itself, or by using that component in conjunction with one or more external Cisco RPMSs.

For more information about RPM, refer to Resource Pool Management at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120t/120t5/rpm1205t.htm

In a Cisco ASAP network, Cisco RPMS enables PPM across multiple UGs, and models customers, services, and regions according to DNIS, trunk, or GW. Cisco RPMS provides support for L2F/L2TP tunnel definition (VPDN access) and tunnel policy management for dial calls.

Note In initial releases of the Cisco ASAP Solution, Cisco RPMS 1.1 is supported for tunnel policy management to provide PPM for dial services only. This includes preauthorization and the ability to configure Cisco RPMS to provide VPDN tunnel definition and policy management.

For further information, see Port Policy Management and Cisco RPMS, page 5-3.

Resource pool management can be configured in a single, stand-alone UG. However, for reasons of scale, Cisco recommends that Cisco ASAP Solution implementations take advantage of a Cisco RPMS (RPMS 1.1 or later).

Note PPM can also be implemented on an AAA server.

For more information about Cisco RPMS 1.1, 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

Cisco Info Center

Cisco Info Center (CIC) is member of the CiscoWorks2000 family. CIC provides a variety of features with respect to fault management and event correlation.

For further information, see Cisco Info Center, page 5-4.

Cisco Internet Performance Manager

Cisco Internet Performance Manager (IPM) is a performance management application that can monitor the performance of a service provider's network, with special application for voice. Cisco IPM provides a variety of features related to VoIP network performance.

For further information, see Cisco Internet Performance Manager, page 5-5.

Element Management Systems

Element management systems (EMSs) are optional components that are used for managing or provisioning other components in the solution.

The following element management systems may be used in the Cisco ASAP Solution:

- Cisco Universal Gateway Manager
- Cisco Voice Manager
- Cisco MGC Node Manager
- Cisco Voice Services Provisioning Tool

Cisco Universal Gateway Manager

The Cisco Universal Gateway Manager (UGM) is an element management system for Cisco UGs. (The Cisco AS5300 is not supported.) Running on a Sun Solaris platform, Cisco UGM provides comprehensive FCAPS (Fault, Configuration, Accounting/Inventory, Performance, and Security) capabilities, for the configuration, management, and maintenance of dial networks. Cisco UGM accesses standards-based information through SNMP (Simple Network Management Protocol), Telnet, and FTP/TFTP.

For further information, see Cisco Universal Gateway Manager, page 5-6.

Cisco Voice Manager

CiscoWorks2000 Voice Manager (CVM) is a web-based management and reporting application for Cisco UGs and GKs. CVM provides basic service provisioning (dial plan management) in voice applications, and integrates with third-party reporting tools for distributed reporting.

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.

For further information, see Cisco Voice Manager, page 5-6.

Cisco MGC Node Manager

Cisco Media Gateway Controller Node Manager (CMNM) is an element management system for the Cisco SC2200 node. CMNM provides a single interface for fault, configuration, and performance management for all network elements within the node.

For further information, see Cisco MGC Node Manager, page 5-8.

Cisco Voice Services Provisioning Tool

Cisco Voice Services Provisioning Tool (VSPT) is a GUI-based tool for provisioning the Cisco SC2200 (Sun Netra) hardware platform. VSPT can bulk load and import provisioning information, and supports incremental provisioning. It can also generate provisioning command scripts, and can be launched directly from CMNM.

For further information, see Cisco Voice Services Provisioning Tool, page 5-8.

RADIUS-Based Platforms

A variety of platforms that use the RADIUS (Remote Authentication Dial-In User Service) protocol are available to support the Cisco ASAP Solution for dial and voice services. This includes authentication, authorization, and accounting (AAA).

RADIUS-based servers perform different functions for dial and voice:

- For dial services, the server maintains end-user (subscriber) information, such as user name and password.
- For (prepaid) voice services, the server maintains end-user information such as credit card number and PIN, in addition to a real-time subscriber rating engine.

In addition, a RADIUS AAA server can be used simply as a place to receive and maintain CDRs (call detail records) from the GWs.

The following RADIUS-based platforms are discussed below:

- Cisco Access Registrar
- RADIUS Proxy Server

Cisco Access Registrar

Cisco Access Registrar (AR) is a RADIUS-compliant access policy server (and proxy server) designed to support the delivery of dial, VoIP, ISDN, and wireless, among other services. Based on Sun Solaris, Cisco AR helps service providers deploy access services by centralizing AAA information while simplifying provisioning and management. AAA RADIUS servers are used, for example, in card services to validate end users on the basis of called number or username and password combination. The AAA interaction occurs directly on the GW.

Version 1.6, recommended for use with the Cisco ASAP Solution, provides policy enforcement support, configuration replication for multiserver deployments, and a number of additional features to simplify administration and troubleshooting.

The Cisco ASAP Solution can use Cisco AR in wholesale dial services as an AAA server or proxy server, or to provide VPDN tunnel definition (without the use of L2TP tunneling) for dial-in data connections.

Features include the following:

- Authentication of users stored in an LDAP (Lightweight Directory Access Protocol) directory

- Retrieval of user/service authorization parameters from an LDAP directory
- Extension points for supporting custom applications or new services
- Proxy RADIUS for support of wholesale dial, remote access outsourcing, and global roaming applications
- IETF tunneling support for standards-based tunneling
- Enforcement of user and group session limits
- Allocation of IP addresses from an IP address pool
- Centralized definition of user and group session limits and IP pools
- Logging to a central syslog server
- Integration with third-party provisioning, billing, management, and operational systems of the service provider's choice

For more information, see Cisco Access Registrar at the following URL:

http://www.cisco.com/warp/public/779/servpro/operate/csm/nemnsw/car/prodlit/index.shtml

RADIUS Proxy Server

When a RADIUS proxy server is used in the wholesale SPs network, the DNIS can be used to authenticate users to one retail ISP or another. This provides a variety of benefits:

- Requests for authorization are forwarded to the retail ISP AAA server.
- The retail ISP maintains the subscriber relationship, authenticating its own users and assigning its own IP addresses.
- Authorization criteria are maintained in a central server, simplifying operations and facilitating scaling.
- The wholesaler is isolated from interacting with the end user.

Billing Systems

Billing systems and the servers that run billing applications will be required.

For a discussion of billing, refer to Understanding and Provisioning AAA Billing, and Establishing Billing Systems for Calling Card Services, in Chapter 3, "Provisioning Shared Support Services," of the *Cisco Wholesale Voice Solution Design and Implementation Guide*.

For a discussion of back-to-back gateways, refer to Back-to-Back GW in Chapter 2, "Solution Architecture," of the *Cisco Wholesale Voice Solution Overview.*

Both documents are available at the following URL:

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

In addition, the Cisco Billing and Measurements Server (BAMS) can be used. 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.

Unified Communications Application Server

Unified communications (UC) servers support unified messaging—the convergence of voice mail, e-mail, and fax. UC servers allow a subscriber to take advantage of store-and-forward delivery, whereby a message recipient has the option of retrieving a message by means of phone, email, or fax at a convenient time. Open Packet Telephony (OPT) architecture is the cornerstone of unified communications.

Caution Initial releases of the Cisco ASAP Solution do not support T.37 store-and-forward fax. Unified communications solutions will be provided by Cisco partners, and will eventually include such applications as voice mail over IP with unified messaging and store-and-forward fax.

TFTP Prompt Server

A prompt server is an optional component that maintains a prompt database for UGs running IVR functionality for applications such as card services. If they are not too big, prompt databases may be stored locally on the UG in flash memory. Larger prompt databases, such as those needed when there are many branded retailers or when many languages must be supported, may be downloaded dynamically as needed from a TFTP prompt server. TFTP servers are generic third-party devices that can be hosted on a wide variety of platforms.

TFTP servers are used to store a variety of files that do not need to reside on a local machine, and that would otherwise take up available limited memory on that machine. These files can be downloaded as needed. Example files include audio (IVR) files, IOS files, and configuration files (including dial peers).

NTP Time Server

Single-source timing is essential in synchronizing timing across multiple time zones. This is especially true where Cisco RPMS, billing applications, and other services are involved. Network Time Protocol (NTP) servers are a recommended source of high-quality timing. NTP provides a common time base for networked routers, servers, and other devices. Synchronized timing enables one to correlate syslog and Cisco IOS debug output to specific events. An NTP-enabled network usually gets its time from an authoritative time source. A Cisco router can provide this function, but more critical timing may require a device such as an atomic clock attached to a time server. NTP then distributes the timing across the network.

Designing a Solution

Overview: Design Issues and Choices

This chapter introduces a variety of issues that must be considered in designing a Cisco ASAP Solution, in particular because this solution provides for a mix of voice and data, as well as specific services.

The following major topics are discussed in this chapter:

- H.323 Network Issues
- Dial Plans and Number Normalization
- Dynamic Call-by-Call Handling
- SS7 Interconnect
- Network Design Guidelines
- Billing and Settlement

H.323 Network Issues

IP telephony networks of any considerable size will require a network signaling protocol such as H.323, SIP, or MGCP to support resource management, call routing, and security, among other features. H.323 is currently the de facto standard required for voice services, although it provides optional support for data and voice. Initial releases of the Cisco ASAP Solution support large-scale H.323 networks only (see Cisco H.323 Gatekeepers and Directory Gatekeepers, page 3-5), although support will later be provided for networks that rely on protocols such as SIP and MGCP. Issues related to the design of H.323 networks are documented in the *Cisco Wholesale Voice Solution Design and Implementation Guide*, available at the following URL:

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

In the that document, Chapter 2, “Provisioning the Gatekeeper Core,” provides a good discussion of H.323 design issues, including the roles of the gateway (GW), gatekeeper (GK), and directory gatekeeper (DGK).

Dial Plans and Number Normalization

Unified Dial Plans

A dial plan is essentially a telephony call routing plan for an IP network. The dial plan is the method by which individual blocks of telephone numbers (technically, E.164 addresses) are assigned to physical facilities, or circuits. For large-scale service provider networks, dial plans consist of the following:

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

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

Note Dial plans for VoIP are well-documented. For additional discussion, including design methodology, refer to Dial Plans and Number Normalization 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

With the data and voice features of UGs, a *unified* dial plan is required, in order to support both voice and dial numbers. A unified dial plan differentiates services on a call-by-call basis.

With the Cisco ASAP Solution, Cisco IOS dial peers are used to build a call routing plan. The designer must be able to associate a DNIS with a service. In this case, the DNIS (**incoming called-number**) is used as the foundation of a dial peer match. If a match is made, the call is handled according to dial-peer parameters; if not, it is simply handled as a dial call. However, a dial access number *must not match* a dial peer, as in the following example for a debit card dial peer but with a DNIS of 4085552000—destined for dial service.

```
dial-peer voice 1 pots
 application debitcard
 incoming called-number 4085551000
 port 1/0:D
```

We do not want the following:

```
dial-peer voice 10 pots
 incoming called-number . <--4085552000 is a dial access number, and must not be matched
 port 1/0
```

Note The software design is such that a failure to match a dial call with a dial peer will automatically cause the dial call to be treated as a modem call.

Number Normalization

Number normalization (or translation) is a term for the prefixing or digit stripping of telephone numbers at the POP GWs. It generates consistent number formats in the core, simplifying GW dial-peer complexity, reducing the number of dial peers, and minimizing prefix configurations on the GKs. Number normalization is performed on the ingress GW before a call enters the VoIP network, and on the egress GW, before the call enters the PSTN. Translation rules and prefixing are applied in accordance with local dialing patterns.

Note For more information about translation rules, including examples, refer to Configuring Translation Rules on the Gateways 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

Dynamic Call-by-Call Handling

In addition to being able to accommodate a variety of different numbering plans, the network designer must be able to map incoming calls to a variety of service applications as appropriate for each call. For example, for a prepaid calling-card service, prompts would have to be provided in, say, Chinese or English, depending upon (for the most part) the home country of the subscriber. To enable a variety of interactive responses, scripts are required.

Call Control Scripts

The Cisco ASAP Solution will use call control scripts written in one of two scripting languages: Cisco TCL IVR (Tool Control Language Interactive Voice Response) scripts are currently supported, whereas VXML (Voice eXtensible Markup Language) scripts will later be supported. Both of these, invoked by dial peer port or DNIS parameters, will play a significant role in the services enabled by UGs, in particular with respect to unified messaging and mobile applications where only voice interaction is practical. Both languages are readily accessible open standards, and provide the following advantages:

- Enable easy service customization.
- Enable rapid application development.
- Use scripts stored on centralized (TFTP) servers for ease of maintenance.
- Offer a wide range of debugging capabilities.

Cisco TCL IVR

IVR consists of simple voice prompting and digit collection to gather caller information in order to authenticate the user and identify the destination. IVR applications can be assigned to ports, or can be invoked on the basis of DNIS. An IP PSTN GW can have a variety of IVR applications to accommodate different services, and different interfaces can be presented to different callers. Cisco TCL IVR uses Tool Control Language scripts to gather information, as well as to process accounting and billing.

Note For more information about Cisco TCL IVR, including a discussion of the TFTP servers required to support the files, refer to Provisioning Services to Support IVR, in Chapter 3, "Provisioning Shared Support Services," of the *Cisco Wholesale Voice Solution Design and Implementation Guide*.

VXML

VXML (also referred to as VoiceXML), a markup language like HTML, is an extension of XML for voice applications. It runs on an HTTP server and enables voice browsers. Voice browsers are similar in function to standard visual browsers, except that they both interpret voice commands and can either issue synthesized audio prompts or play prerecorded digital audio files. They can also interpret DTMF tones from a keypad.

Caution VXML is not supported in initial releases of the Cisco ASAP Solution.

Note The VXML specification is available at the following URL:
http://www.w3.org/TR/voicexml/

The VoiceXML Forum (sponsored by IEEE-ISTO) provides additional information at the following URL:
http://www.voicexml.org

SS7 Interconnect

Where SS7 must be supported, the Cisco ASAP Solution relies on the Cisco SS7 Interconnect for Voice Gateways Solution. That solution is a distributed system that provides SS7 connectivity for H.323 VoIP access gateways, by using the Cisco Signaling Controller (also known as the Cisco SC2200) and access gateways as a bridge from the H.323 IP network to the PSTN. The Cisco SS7 Interconnect for Voice Gateways Solution interacts over the IP network with other Cisco H.323 VoIP access gateways; it can also interoperate with H.323 endpoints by using non-SS7 signaling, as in ISDN PRI and channelized T1.

For the most current information about SS7 connectivity as it relates to the Cisco ASAP Solution, refer to the discussion of the Cisco SS7 Interconnect for Voice Gateways Solution, Release 1.1. That solution is described in detail at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/access/sc/rel7/soln/voip11/index.htm

For an example architecture, 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

The same Cisco SC2200 node can be used to support both voice and dial traffic, in either distributed or centralized architectures. Redundancy is inherent in SS7 signaling architectures. The Cisco SC2200 hosts can either be colocated with the GWs, or distributed, so that the Cisco SC2200s are remote with respect to the GWs and the SLTs are remote with respect to the Cisco SC2200s. In any architecture, however, the network must meet requirements for delay, QoS, and loss.

Network Design Guidelines

This section discusses a variety of principles that must be considered in designing a Cisco ASAP Solution network. The guidelines cover the following general areas:

- Guidelines for Individual Components
- Solution Resilience
- Traffic Engineering

Guidelines for Individual Components

The following discusses design issues that relate to GWs, GKs, and Cisco SC2200 nodes, respectively.

Guidelines for Gateways

With respect to GWs, in a truly mixed environment, it is important to design to universal port numbers. Use enhanced call admission control (see Call Admission Control and RSVP, page 5-2) to ensure the availability of resources in GWs and across the network.

Guidelines for Gatekeepers and Directory Gatekeepers

With respect to GKs, in a voice-only environment, use DGKs to minimize the need to manage configurations on individual GWs, while also simplifying expansion.

Note The above issue is discussed 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

Guidelines for Cisco SC2200 Nodes

With respect to a Cisco SC2200 node in a mixed environment, you must take care to accommodate both voice and dial calls. There are two optimization models: one for simultaneous calls, the other for calls per second (CPS). Deciding on which parameter to optimize will depend on understanding your statistical traffic types.

Caution 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. For a general discussion of these issues that will assist you in understanding the tradeoffs, see Optimizing the Performance of the Cisco SC2200, page 2-4.

Solution Resilience

Resilience in networks is achieved through general redundancy—in routes, physical connections, solution components, and uninterruptible power supplies (UPSs), as well as in the software that provides intelligent fault detection and quick failover to healthy components. In SS7 applications, redundant signaling equipment (Cisco SC2200 signaling controllers, Cisco SLT) is required, as are other components throughout the SS7 network.

In large GK-deployment networks, there are three principle ways to provide resilience through fault tolerance (also known as continuous service):

- Use Cisco HSRP (Cisco's Hot Standby Routing Protocol).

  This provides fault tolerance at the GK and DGK level, but is especially effective when applied at the DGK level.

- Use alternate GKs.

  This allows a GW to use up to two alternate GKs as a backup in case a primary GK fails. The GWs are configured to register to a primary and an alternate GK. If the primary GK fails, the alternate GK can then be used for call routing.

- Use an alternate DGK.

  This provides coverage while HSRP failover detection is taking place. Here, local GKs are configured to point to an alternate DGK, which in turn can be used to back up an HSRP DGK pair.

Note For an extended discussion of the above fault-tolerance methods, refer to 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

Caution In a Cisco ASAP Solution, consideration must be given to providing redundancy in components other than principal network components—TFTP servers, PPM and AAA servers, billing and accounting application servers, and the like.

Traffic Engineering

A variety of issues must be considered with the advent of UGs and universal service. Some practical guidelines are presented below.

Convergence and Migration Considerations

Although building a network from scratch offers many advantages, the practical case is that networks expand upon their existing base. With the Cisco ASAP Solution, this means that dial services will be added to existing voice services, or that voice services will be added to existing dial services.

Adding Dial to a Voice Network

In adding dial services to an existing voice network, realize that the longer hold times and larger packets associated with data connections will increase the demand for bandwidth. It becomes important to ensure that voice quality is maintained through quality of service (QoS) monitoring and applications.

Adding Voice to a Dial Network

The shorter call hold times and smaller packets associated with voice place greater demands on CPUs throughout the network. In addition, maintaining voice QoS demands tightly controlled delay, loss, and jitter parameters.

Achieving End-to-End Quality of Service

Given that latency and other characteristics of burdened traffic in a network can be forgiving with respect to data, the primary objective of any network must be to achieve and maintain QoS for voice traffic. The following general guidelines must be adhered to:

- Ideally, there should be no lost packets. The default G.729 codec requires less than 1% packet loss.
- Keep end-to-end delay less than 150 msec.
- Minimize jitter. Jitter buffers add to end-to-end delay.

Contention

Contention is a collision of demands, and takes a variety of forms: over resources (CPU, DS0), as well as over links (between voice and voice and voice and data calls).

Contention issues cannot be ignored in a network design. Among the contention domains, contention can occur at the UG/PSTN interface, the UG/network edge interface, the edge/core (GK to DGK) interface, and in the core itself. At the link level, voice can contend with data, but voice can also contend with voice if overall bandwidth is not sufficient.

Table 4-1 lists the contention types, as well as their remedies, all of wich are Cisco IOS features. The features are introduced briefly below.

Note These features are discussed in greater detail in Chapter 3, "Using Management and Shared Support Services," of the *Cisco ASAP Solution Implementation Guide*.

Table 4-1 Contention Types and Remedies

Contention Type	Remedy	Where Applied
Resource	Call admission control (CAC)	GW
Voice/voice	Resource Reservation Protocol (RSVP)	GW, access network
	RSVP-based CAC	
Voice/data	IP precedence	GW
	Low latency queuing (LLQ)	GW, access network, core
	RSVP/LLQ integration	GW, access network

Call Admission Control

When too much data traffic burdens a particular network link, techniques such as queuing, buffering, and packet dropping can relieve the congestion. The extra traffic is simply delayed until the interface is once again available, or, if packets are dropped, either the protocol or the end user initiates a timeout and requests retransmission.

With real-time traffic such as voice, this is not acceptable. Both latency and packet loss jeopardize the QoS expected by users. For delay-sensitive traffic such as voice, it is better to deny network traffic at the outset under certain conditions. Call admission control (CAC) is a *set* of voice-specific mechanisms designed to do this.

CAC, administered on the GW or NAS, ensures that resources available before the call is answered or completed. There are two forms of CAC: basic and enhanced. The enhanced version has capabilities for monitoring more UG and network resources. Table 4-2 summarizes the features in each form of CAC.

Note For more information and provisioning details, refer to Chapter 3, "Using Management and Shared Support Services," of the *Cisco ASAP Solution Implementation Guide*.

Table 4-2 Basic and Enhanced CAC

Basic	Enhanced
PSTN side: • On UGs, monitors DS0s, DSPs, and HDLC framers • Calls not delivered/accepted if any set of required resources are all in use • Enabled by default	*UG resources*: • Monitors UG health resources • Has call treatment options • Has call rate restrictions
Network side: • On UG, monitors DS0s and DSPs • UG uses RAI to inform GK when threshold is exceeded • Enabled through CLI	*Network resources*: • Monitors end-to-end bandwidth • Monitors end-to-end voice quality

Resource Reservation Protocol

Resource Reservation Protocol (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-Based CAC

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.

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.

Low Latency Queuing

Low latency queuing (LLQ) is another remedy for voice/data contention. The Cisco Low Latency Queuing 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.

RSVP/LLQ Integration

RSVP uses weighted fair queuing (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.

Additional Traffic Engineering Issues

There are a variety of traffic-engineering challenges posed by a Cisco ASAP Solution network, the majority of which are related to varying bandwidth throughout the network. These topics are listed below.

Note These issues are discussed in Chapter 3, "Using Management and Shared Support Services," of the *Cisco ASAP Solution Implementation Guide*.

- 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 Interface
- Core Issues

Billing and Settlement

Voice services and even some data services will require reliable billing mechanisms to account for call start and stop times across the various call legs, or definable sections of a call's path. This is especially important in cases where multiple service providers are involved and billing must be partitioned, or settled, according to who "owns" the call legs that are traversed. The features available in the H.323 standard for packet telephony provide for billing from the GW by using the accounting component of AAA/RADIUS capabilities.

Note For additional information, refer to Understanding and Provisioning AAA Billing 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

Solution Management

The success of a Cisco ASAP Solution relies largely on ensuring that quality of service (QoS) is maintained once voice and dial traffic is combined. This requires an understanding of the techniques and applications available for the following key areas:

- Resource Management

  Includes maintaining QoS by avoiding contention, and managing voice and data traffic.

- Additional Network Management Tools

  Includes such applications as Cisco Info Center and Cisco Internet Performance Monitor.

- Element Management Systems

  Includes managing GWs; configuring and managing VoIP ports, dial peers and dial plans; and managing SS7 components, among many other features.

Resource Management

Resource management is essentially the management of traffic, with special application for VoIP telephony where quality of service, or QoS, must be maintained. The following sections briefly introduce several techniques, both H.323 and Cisco IOS based, to ensure QoS:

- Ensuring Quality of Service
- Call Admission Control and RSVP
- IP Precedence
- Port Policy Management and Cisco RPMS

Note These techniques are discussed in greater detail in Chapter 3, “Using Management and Shared Support Services,” in the *Cisco ASAP Solution Implementation Guide*.

Ensuring Quality of Service

The following are some key principles to adhere to in order to ensure QoS:

- Separate signaling traffic from user traffic.

  The first priority is to answer the call!

- Separate voice traffic from data traffic.

  Because voice demands tightly controlled delay, loss, and jitter, it is necessary to prevent the destructive interaction of the two traffic types.

- Schedule signaling and voice traffic over dial traffic.

In short, give precedence to voice communications—once again. In the voice traffic component of a Cisco ASAP Solution, it is essential that customers receive the same quality of service, or QoS, that they receive with basic PSTN services. Unlike data services, VoIP, being a real-time service, is extremely sensitive to such factors as bandwidth and delay. A variety of remedies are introduced in the sections that follow.

Call Admission Control and RSVP

When too much data traffic burdens a particular network link, techniques such as queuing, buffering, and packet dropping can relieve the congestion. The extra traffic is simply delayed until the interface is once again available, or, if packets are dropped, either the protocol or the end user initiates a timeout and requests retransmission.

With real-time traffic such as voice, this is not acceptable. Both latency and packet loss jeopardize the QoS expected by users. For delay-sensitive traffic such as voice, it is better to deny network traffic at the outset under certain conditions. Call admission control (CAC), a generic term, is a *set* of voice-specific mechanisms designed to do this.

RSVP and RSVP-Based CAC

RSVP (Resource Reservation Protocol) is an IETF standard designed to support resource (such as bandwidth) reservations through networks of varying topologies and media. The Cisco Resource Reservation Protocol feature is an enhancement to CAC that ensures QoS in Cisco ASAP Solution networks where H.323 is used.

Note CAC, both basic and enhanced, is discussed in greater detail in Chapter 3, "Using Management and Shared Support Services," in the *Cisco ASAP Solution Implementation Guide*.

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

Low Latency Queuing

Low latency queuing (LLQ) is another remedy for voice/data contention. LLQ is a feature that is supported by the Cisco Resource Reservation Protocol. The Cisco Low Latency Queuing 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.

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 GW edge interfaces, both voice and modem.

Port Policy Management and Cisco RPMS

Port policy management (PPM) is the ability to aggregate ports as a shared pool—either in a single GW or across stacks of multiple GWs. PPM is a key component of port wholesaling, as it allows ports to be allocated dynamically before the call is answered. This allows wholesale access service providers (ASPs) to lease voice and dial ports *virtually* to customers, and also to enforce SLAs by restricting port use according to port policy.

Caution In initial releases of the Cisco ASAP Solution, port policy management is supported for dial services only.

For example, consider a wholesale ASP who wants to host a dial-only SP (such as MSN), a voice-only SP (such as DialPad), and a voice and dial SP (such as AOL). The following basic activities would then be implemented:

- Wholesale ASP pools ports across universal GWs.
- Ports are allocated on demand to customers and services.
- Policies on port use are established and enforced on a per-GW or per-POP basis, or across the entire network.

PPM provides multiple benefits to the wholesaler:

- Allows wholesaler to manage ports efficiently, lowering cost.
- Guarantees SLAs without the need to dedicate ports, trunks, or GWs.
- Enforces limits on port use before the call is accepted, preventing ports from being tied up.
- Prevents degradation in service that can result from customer oversubscription.
- Preserves quality of experience of subscriber.

The Cisco Resource Policy Management (RPM) feature, critical to dial solutions, is a port policy management (PPM) feature that resides on the UG, but that can also be implemented through a Cisco RPMS. Port policy management is essential to the Cisco ASAP Solution.

Note PPM can also be implemented on an AAA server.

The Cisco RPM feature enables wholesalers to aggregate their dial resources across multiple NASs (UGs), and allocate subsets of these resources to retail ISPs. RPM can be achieved by using the RPM component of the resource pooling solution on the NAS itself, or by using that component in conjunction with one or more external Cisco RPMSs.

The following are key components of the RPMS feature:

- Enforcement of SLAs between a wholesale SP and a retail ISP prior to call acceptance
- Soft and hard limits for port usage by the retail ISP
- Accounting through special tagging for port usage exceeding a soft limit
- Grouping of physical resources at the UG (for speech, digital, v.110 traffic)
- Resource assignment and configuration (modem speed, compression) per retail ISP
- Call screening and call rejection treatment (busy, no answer, channel not available)
- VPDN management, through load balancing among LNSs (L2TP network servers), and through tunnel limits per LNS
- Real-time reports through a Web GUI

Note For additional information, refer to *Cisco Resource Management Pool 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

Also refer to Resource Pool Management at the following URL: http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120t/120t5/rpm1205t.htm

RADIUS PPM Server

A RADIUS-based PPM server can also be used for preauthentication. See RADIUS-Based Platforms, page 3-12.

Additional Network Management Tools

The following are additional network management tools that can be used in conjunction with a Cisco ASAP Solution:

- Cisco Info Center
- Cisco Internet Performance Manager

Cisco Info Center

Cisco Info Center (CIC) is another member of the CiscoWorks2000 family. CIC provides the following features with respect to fault management and event correlation:

- Optimizes fault management by reducing alarm information overload through “de-duplication” and fault correlation; this enables faster problem solving and better operations scaling.
- Flexibly manages and monitors faults in multivendor, multitechnology, and multiservice environments.
- Correlates faults received from multiple sources, such as SNMP traps and syslog events.

- Supports distributed operational environments, to do such things as the following:
  - Reduce the number of NOCs (network operations centers).
  - Provide centralized and regional monitoring.
  - Eliminate costly, inefficient “console farms” of scrolling alarms.
- Translates faults and events into actions, to do such things as the following:
  - Page key maintenance personnel.
  - Issue trouble tickets.
  - Send alarms for critical events.
- Provides a distributed, redundant architecture, for scaling and reliability.

The most current version is Release 2.0. For additional information, refer to *Cisco Info Center 2.0 Release* at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/info_ctr/2_0_0/index.htm

Cisco Internet Performance Manager

Cisco Internet Performance Manager (IPM) is a performance management application that can monitor the performance of a service provider’s network with special application for voice. Cisco IPM provides the following features related to network performance:

- Provides real-time and historical network-performance reports on VoIP characteristics such as the following:
  - Latency
  - Jitter
  - Packet errors
  - Packet loss for all available IP paths
- Measures network performance on a hop-by-hop basis, to do such things as the following:
  - Pinpoint latency and jitter causes.
  - Reduce problem isolation and resolution time.
- Generates traps based on response-time thresholds, to provide real-time alerting of potential problems.
- Works with Cisco IOS Service Assurance Agent (SAA) to support service level measurement.

Element Management Systems

Element management systems (EMSs) are optional components that are used for managing or provisioning other components in the solution.

Note CVM 2.0.2 provides limited provisioning support and is currently the only EMS supported by the Cisco ASAP Solution.

The following element management systems are considered the principal EMSs for use in the Cisco ASAP Solution:

- Cisco Universal Gateway Manager
- Cisco Voice Manager
- Cisco MGC Node Manager
- Cisco Voice Services Provisioning Tool

Cisco Universal Gateway Manager

The Cisco Universal Gateway Manager (UGM) is an element management system for Cisco UGs. Running on a Sun Solaris platform, UGM provides comprehensive FCAPS (Fault, Configuration, Accounting/Inventory, Performance, and Security) capabilities, for the configuration, management, and maintenance of dial networks.

UGM provides the following features:

- Autodiscovery (of new UGs and subchassis components) and inventory management
- Fault management through an event browser and network map, with UG availability and alarm states
- Management of configuration files and Cisco IOS images, including the distribution of Cisco IOS and DSP images
- Historical and snapshot performance monitoring of the dial network, including chassis, modems, and each T1/E1 or T3 interface
- Role-based security, through read only, read-write, and read-write-administrative privileges

User documentation for the Cisco UGM is available at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/ugm/index.htm

Cisco Voice Manager

CiscoWorks2000 Voice Manager (CVM) Version 2.0.2 is an element management system that provides the following features:

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

CiscoWorks2000 Voice Manager (CVM) Release 2.0.2 supports performance and statistical reporting for voice services within the Cisco ASAP Solution. CVM is a client/server, web-based solution to managing the VoIP functionality of the UGs used in the solution. CVM allows you to do the following:

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

Note 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.

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

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

Key Features in CVM

CVM is a client/server, web-based voice management solution. The following list describes some of the key features of CVM:

- *Voice port management*—Manage the configuration of FXO, FXS, E&M, and ISDN configurations in single or batch mode.
- *Dial plan management*—Create and manage local dial plans and VoIP, VoFR, and VoATM network dial plans.
- *Report generation*—See the Telemate.net Quickview documentation for complete details of the reports you can generate.
- *Multiple platform support*—CVM clients can run in web browsers running Windows 95, Windows NT, or Solaris platforms.
- *Integration with CiscoWorks 2000 CD One*—CVM is integrated with CiscoWorks2000 CD One, which provides a common platform for running different applications that manage a wide variety of router functions.
- *Scalability*—CVM can scale to support combinations of the following voice-enabled Cisco routers: Cisco 1700 series, Cisco 2600 series, Cisco 3600 series, Cisco MC3810 multiservice access concentrator, Cisco AS5300 series universal access server, and Cisco 7200/7500 series.

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

CVM's support for SNMP includes trap viewing and forwarding. CVM 2.0.2 can receive and collect traps from GWs through SNMP. Traps can be forwarded to Cisco Info Center (CIC) for event correlation.

Note CVM is a stand-alone product that is not appropriate to the scaling needs of large-scale service providers. Although CVM can be used on a POP basis for small to medium service providers, it is not suitable for wholesale providers. It is used primarily with a polling application. In order to provide an effective distributed reporting solution, CVM requires integration with a third-party partner.

More information about Cisco Voice Manager is available at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/voicemgr/index.htm

Cisco MGC Node Manager

Cisco Media Gateway Controller Node Manager (CMNM) is the element management system for the components of a Cisco MGC node, also known here as an SC2200 node.

Note In the Cisco Open Packet Telephony (OPT) architecture, MGC is a generic term for the call-control functional layer.

Cisco CMNM provides fault, configuration, accounting, and performance management.

Caution Switches are 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.

For more information about Cisco CMNM, refer to the *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/

Cisco Billing and Measurements Server

Cisco CMNM also incorporates the Cisco Billing and Measurements Server, or BAMS. BAMS collects, formats, and stores billing and measurements data from the Cisco MGC (Cisco SC2200 node). BAMS-formatted data can then be processed by a billing system and other measurement collection and reporting systems.

For more information, 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.

Cisco Voice Services Provisioning Tool

Cisco Voice Services Provisioning Tool (VSPT) can also be deployed as an integrated component of Cisco CMNM. Cisco VSPT provides a configuration and provisioning graphical user interface for the Cisco SC2200 host as well as for the Cisco BAMS component.

Note Cisco VSPT can also be deployed as a stand-alone application.

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

ANI Automatic Number Identification

AR Cisco Access Registrar

ARJ Authorization Reject

ARP Authorization Permit

ASP Application service provider

ARQ Authorization Request

B

BHCA busy hour call attempts

BAMS Cisco Billing and Measurements Server

C

CAS channel-associated signaling

CBWFQ class-based weighted fair queuing

CDR call detail record

CIC Cisco Info Center

CLI command line interface

CMNM Cisco Media Gateway Controller (MGC) Node Manager

CO central office

CORBA	Common Object Request Broker Architecture
CPS	calls per second
CPU	central processing unit
CSR	customer service record
CVM	CiscoWorks2000 Voice Manager

D

DGK	directory gatekeeper
DHCP	Dynamic Host Configuration Protocol
DNIS	Dialed Number Identification Service
DRQ	Disconnect Request
DSP	digital signal processor
DTMF	dual tone, multifunction

E

EMS	element management system
EO	end office
ETSI TIPHON	European Telecommunications Standards Institute Internet Protocol Harmonization over Networks

F

FCAPS	Fault, Configuration, Accounting, and Performance Management System

G

GK	gatekeeper
GKRCS	gatekeeper-routed call signaling
GKTMP	GateKeeper Transaction Message Protocol—a Cisco-proprietary protocol that allows third-party applications to influence the operation of the IOS GK
GW	gateway

H

HSRP Hot Standby Router Protocol—used to ensure GK fault tolerance

I

IETF Internet Engineering Task Force

IMT intermachine trunk

IPM Cisco's Internetwork Performance Monitor

ISL Inter-Switch Link

ISP Internet service provider

ISUP ISDN User Part

ITSP Internet telephony service provider

IVR interactive voice response

IXC interexchange carrier—a regulated U.S. Class 4 carrier that is often a wholesale customer

L

L2F Layer 2 Forwarding Protocol

L2TP Layer 2 Tunnel Protocol

LAC L2TP access concentrator

LCR least-cost routing

LDAP Lightweight Directory Access Protocol

LEC local exchange carrier

LLQ low latency queueing

LNS L2TP network server

M

MF multifrequency

MGC Media Gateway Controller; see VSC

MGCP Media Gateway Control Protocol

MIB Management Information Base

N

NAS network access server

NI-2 National ISDN version 2—a BRI circuit

NMS network management system

NOA Nature of Address

NOC network operations center

NTP Network Time Protocol

O

OGW originating gateway

OLO other local operators; other licensed operator

OSP Open Settlements Protocol

OSS operations support system

OPT Open Packet Telephony

P

PCM pulse code modulation

PDF Portable Document Format

PIAFS Personal Handyphone Internet Access Forum Standard

PIN personal identification number

POP point of presence

POTS plain old telephone service

PPM port policy manager; port policy management

PSTN public switched telephone network

PTT Post, Telephone, Telegraph—a government-mandated or -operated national telephony carrier

Q

QoS quality of service

R

R2 type of CAS used widely in places other than North America

RADIUS Remote Access 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 redundant link manager

RPM resource pool management

RPMS Cisco Resource Pool Manager Server

RRQ Registration Request

RSVP Resource Reservation Protocol

RTP Real-Time Transport Protocol

RTSP Real-Time Streaming Protocol— for controlling the streaming of RTP packets from a storage source

S

SAA Cisco Service Assurance Agent

SC signaling controller—a Cisco SC2200 signaling gateway that converts SS7 to a backhauled NI-2 protocol to gateways

SGCP Simple Gateway Control Protocol

SIP Session Initiation Protocol

SLA service level agreement

SLT signaling link termination—a Cisco 2611 machine capable of terminating SS7 at the MTP2 layer and backhauling MTP3 (and up) to the SC2200 or virtual switch controller (VSC)

SNMP Simple Network Management Protocol

SS7 Signaling System 7

SSL secure socket layer

T

TAC Technical Assistance Center

TCL Tool Command Language

TDM time-division multiplex; time-division multiplexing

TFTP Trivial File Transfer Protocol

TGW terminating gateway

TSI time slot interchange

U

UC unified communications

UDP User Datagram Protocol

UG universal gateway

UGM Cisco Universal Gateway Manager

UP universal port

UPS uninterruptible power supply

URL uniform resource locator

URQ Unregistration Request

V

VPDN virtual private data (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; also referred to as an MGC

VSPT Cisco Voice Services Provisioning Tool

VXML Voice eXtensible Markup Language (VoiceXML)

W

WFQ weighted fair queuing

WIC WAN interface card

INDEX

A

access VPN 3-7

application server 3-6

autodiscovery 5-6

B

basic wholesale dial network architecture (figure) 2-3

basic wholesale voice network architecture (figure) 2-2

billing 4-9

buffering 5-2

C

CAC 1-4, 4-7

call admission/blocking 3-6

call routing 3-6

  destination E.164 addresses 3-6

CBWFQ 5-3

CDR

  RADIUS server 3-12

  reports 3-6

CIC (Cisco Info Center) 3-11, 5-4

Cisco 2600 3-2

Cisco 3660 3-2, 3-5

Cisco 5500 switch 5-8

Cisco 7200 3-2, 3-5

Cisco 7200 VXR 3-3

Cisco 7200 VXR broadband services aggregator 3-7

Cisco Access Registrar 3-9, 3-12

Cisco AS5300 vii, 3-5

Cisco AS5350 3-2

Cisco AS5400 1-1, 3-2, 3-3

Cisco AS55350 1-1

Cisco AS5800 vii, 3-5

Cisco AS5850 1-1, 3-5

Cisco ASAP Solution

  benefits 1-1

  defined vii, 1-1

Cisco ASAP Solution architecture (figure) 1-3

Cisco Billing and Measurements Server 3-9, 3-13, 5-8

Cisco Catalyst 5000 series 3-3, 3-8, 5-8

Cisco Catalyst 6000 series 3-3, 3-8, 5-8

Cisco Catalyst switches 3-3

Cisco dial-only gateways, interface modules, and supported signaling types (table) 3-5

Cisco HSRP 4-6

Cisco Info Center 3-9, 5-1, 5-4, 5-7

Cisco Internet Performance Manager 3-9, 5-5

Cisco Internet Performance Monitor 5-1

Cisco IOS Service Assurance Agent 5-5

Cisco Low Latency Queueing feature 4-9

Cisco Media Gateway Controller Node Manager 3-12, 5-8

Cisco MGC Node Manager 3-9

Cisco Resource Policy Management 5-3

Cisco Resource Pool Management 3-9

Cisco Resource Pool Management Server 3-9

Cisco Resource Pool Managment Server 3-8

Cisco Resource Reservation Protocol feature 5-2

Cisco RPM 3-10

Cisco RSVP Support for Low Latency Queuing feature 4-9

Cisco SC2200 3-2, 3-6, 4-4

Cisco SS7 Interconnect for Voice Gateways 3-2

Cisco SS7 Interconnect for Voice Gateways 1.1 3-6

Cisco SS7 Interconnect for Voice Gateways Solution 4-4

Cisco SS7 signaling link termination (SLT) systems 3-2
Cisco T.38 Real-Time and Never-Busy Fax Service 2-16
Cisco TCL IVR 4-3
support for 1-6
Cisco Universal Gateway Manager 3-9, 3-11
Cisco universal gateways, interface modules, and supported signaling types (table) 3-4
Cisco Voice Manager 3-9
Cisco Voice Manager (CVM) 3-11, 5-5
Cisco Voice Services Provisioning Tool 3-9, 3-12, 5-8
Cisco Wholesale Voice Solution Design and Implementation Guide ix, 4-10
Cisco Wholesale Voice Solution Overview ix
CiscoWorks2000 3-11
CiscoWorks2000 Voice Manager 5-6
class-based weighted fair queuing 4-9
components
additional (third-party) for shared services (table) 3-9
major (Cisco) components (table) 3-2
third party (shared services) components (table) 3-8
contention 4-7
contention types and remedies (table) 4-7
CORBA 3-9
CVM 3-11, 5-5
element management 3-11, 5-6
performance and statistical reporting 5-6

D

database
prompt 3-14
delay 4-7, 5-2
dial and wireless data (figure) 2-4
dial feature card 3-4
dial-only service 3-4
dial peer
POTS and VoIP 4-2
dial plan 4-2
unified 1-4
DNIS 4-2
document
release of vii
DSP resource 2-15

E

E.164
address 3-6, 4-2
address block 4-2
EMS
Cisco Voice Manager 3-11, 5-5
end office 2-1
event correlation 5-7

F

fax
service 2-16
store-and-forward 3-14
T.38 fax relay 1-5, 3-1
FCAPS 3-9
features and services enabled by the Cisco ASAP Solution (table) 1-5
figures
Basic Wholesale Dial Network Architecture 2-3
Basic Wholesale Voice Network Architecture 2-2
Cisco ASAP Solution Architecture 1-3
Dial and Wireless Data 2-4
Long-Distance Toll Bypass 2-11
Migration from Legacy and PSTN Services 2-14
TDM Switching 2-14
Unified Communications 2-12

G

G.168 3-1
G.711 1-5, 3-1
G.723.1 1-5, 3-1

G.729
codec 4-7
G.729a 1-5, 3-1
GKTMP
and application servers 3-6

H

H.323
gateway 3-6
GKs and DGKs 3-5
HDLC framer 4-8
home gateway 3-7

I

IPM 3-11, 5-5
IP precedence 4-7, 4-9, 5-3
IVR 1-6
files 3-14
prompt server 3-14
TDM switching 2-15

J

jitter 4-7, 5-2

L

L2F 3-7
L2TP 3-7
L2TP network server 3-7
LDAP 3-12
LLQ 4-7, 4-9, 5-3
load balancing 5-4
long-distance toll bypass (figure) 2-11
loss 5-2
LRQ
RAS messages 3-6

M

major components of the Cisco ASAP Solution (table) 3-2
messages
LRQ RAS
routing to other domains 3-6
registration and unregistration (RRQ/URQ) 3-6
message URL http
//www.cisco.com/univercd/cc/td/doc/cisintwk/ita/index.htm x
//www.cisco.com/univercd/cc/td/doc/product/access/sc/rel7/soln/wv_rel1/index.htm ix
MGC 5-8
MGCP 1-4, 4-1
Migration from Legacy and PSTN Services (figure) 2-14
modem (V.92) 1-5
MTP 3-7

N

NAS 3-3
network operations center 5-5
network timing protocol 3-14
NMS 3-10
NOC 5-5
number normalization 4-3
number translation 3-6, 4-3

P

packet dropping 5-2
PIAFS 3-1
polling 5-7
port policy management 1-4, 5-3
preauthentication 5-4

PRI grooming 2-14
prompt
  database 3-14
  server 3-14
proxy server 3-13

Q

QoS 4-6
queuing 5-2

R

RADIUS
  and security 3-6
RAI 3-6, 4-8
  resource management 3-6
redundancy 4-6
registration
  and unregistration (RRQ/URQ) messages 3-6
reporting 5-6
Resource Reservation Protocol 4-7
retailing 1-1
RPM 5-3
RPMS 3-8
RSVP-based CAC 4-7

S

SAA 5-5
server
  application 3-6
  prompt 3-14
  RADIUS 3-6
  TFTP 3-14
SIP 1-4, 4-1
SLA 1-2, 1-5, 5-3
  and Cisco RPMS 1-6
SNMP
  traps 5-4, 5-6
solution
  additional shared services (third-party) components (table) 3-9
  components
    major (Cisco) components (table) 3-2
    third party (shared services) components (table) 3-8
SS7
  and Cisco SC2200 3-7
syslog 3-10
  events 5-4
  server 3-13

T

T.37 store-and-forward fax 3-14
T.38 fax relay 1-5, 3-1
tables
  Cisco Dial-Only Gateways, Interface Modules, and Supported Signaling Types 3-5
  Cisco Universal Gateways, Interface Modules, and Supported Signaling Types 3-4
  Contention Types and Remedies 4-7
  Features and Services Enabled by the Cisco ASAP Solution 1-5
  Major Components of the Cisco ASAP Solution 3-2
  Voice and Data Features of the Universal DSP 3-1
TCL 1-6
Tcl 1-6
TDM
  voice GWs 3-3
TDM switching (figure) 2-14
TFTP server 3-14
toll bypass 2-11
tones
  DTMF 4-4
  test 2-14
translation
  number translation 4-2

traps 5-4, 5-6, 5-7

TSI 2-15

tunnel

limits 5-4

VPDN 3-7

U

unified communications (figure) 2-12

unified communications server 3-14

unified dial plan 1-4

unified messaging 2-13

Universal Port DSP 1-1

universal port DSP 3-1

V

V.110 3-1, 5-4

V.120 3-1

V.42 1-5

V.44 3-1

V.90 1-5, 3-1

V.92 1-5, 3-1

voice and data features of the universal DSP (table) 3-1

VoiceXML 4-4

VPDN tunnels 3-7

VPN 3-7

VXML 1-6, 4-4

W

Weblink Preferences ix

WFQ 4-9

wholesaling 1-1