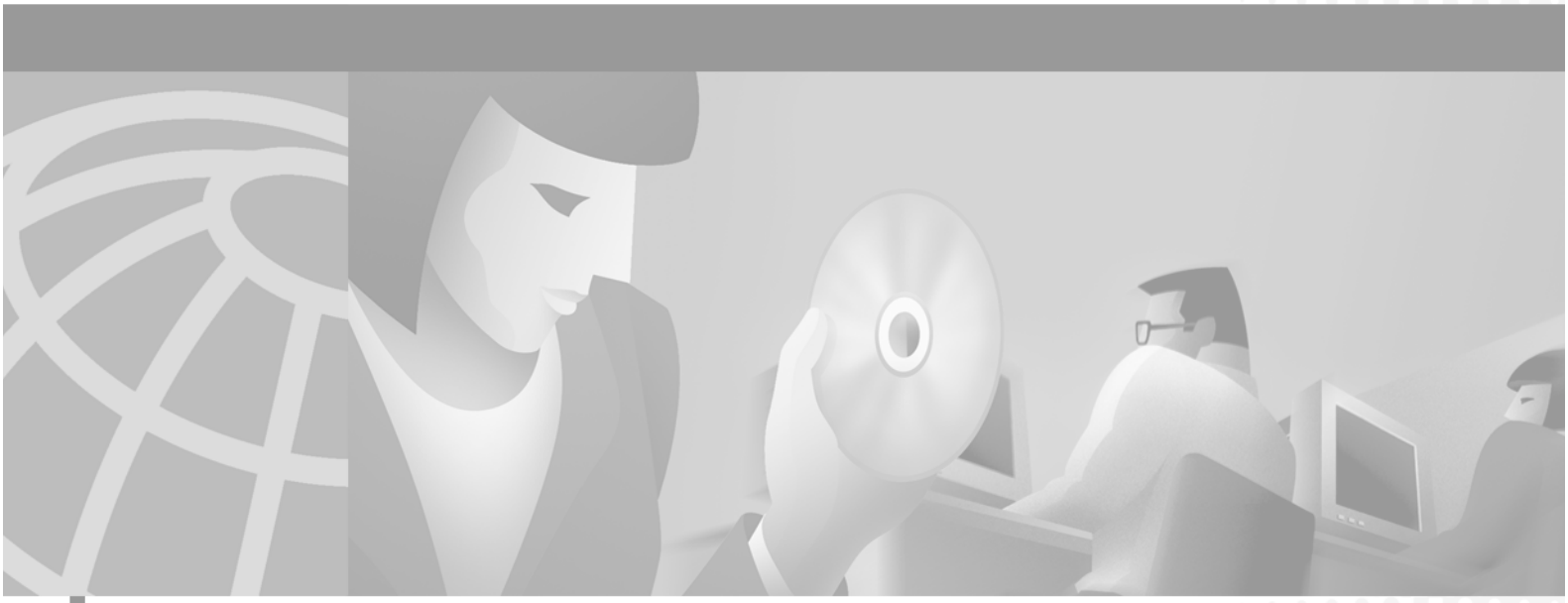
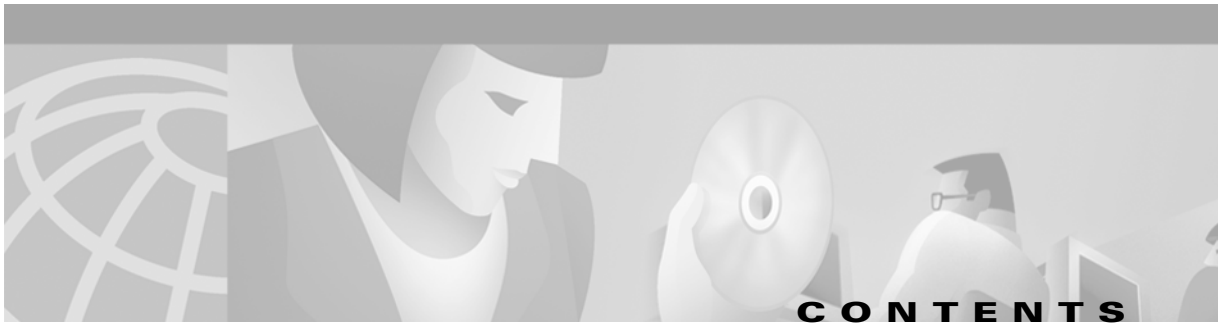
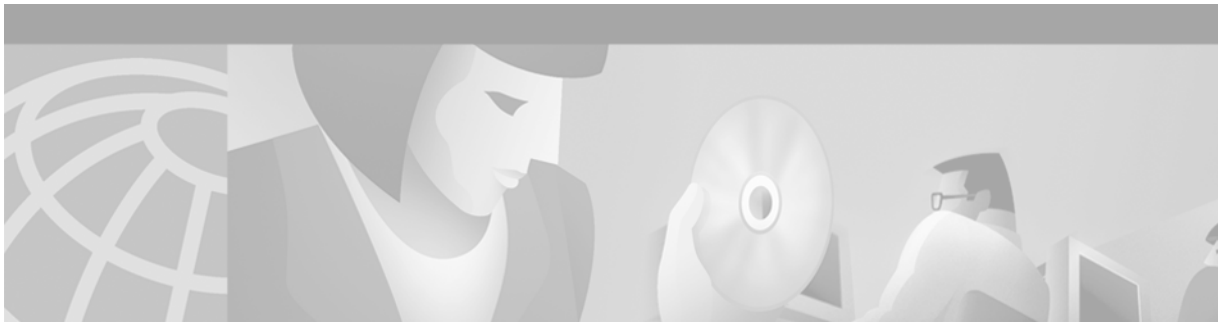


Cisco SS7 Interconnect for Voice Gateways Solution Overview

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



CONTENTS



Preface

This preface describes the objectives, audience, organization, and conventions of the Cisco SS7 Interconnect for Voice Gateways Solution. This document points to related publications and describes online sources of technical information.

Document Objectives

The Cisco SS7 Interconnect for Voice Gateways Solution provides SS7 connectivity for voice gateways by using the Cisco signaling controller as a protocol translator to control the gateway through the ISDN Q.931 protocol.

This guide is designed to provide you with an overview of the Cisco SS7 Interconnect for Voice Gateways Solution and brief information about its components. This guide describes initial site preparation and implementation information with pointers to detailed hardware installation and software configuration documentation.

Audience

This document is part of a suite of documents for the following users. See the "Cisco SS7 Interconnect for Voice Gateways Solution Documentation Suite" section.

- Component installers—Who have experience installing telecommunications equipment and cables, and experience installing data communications equipment and cabling.
- 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.

Document Organization

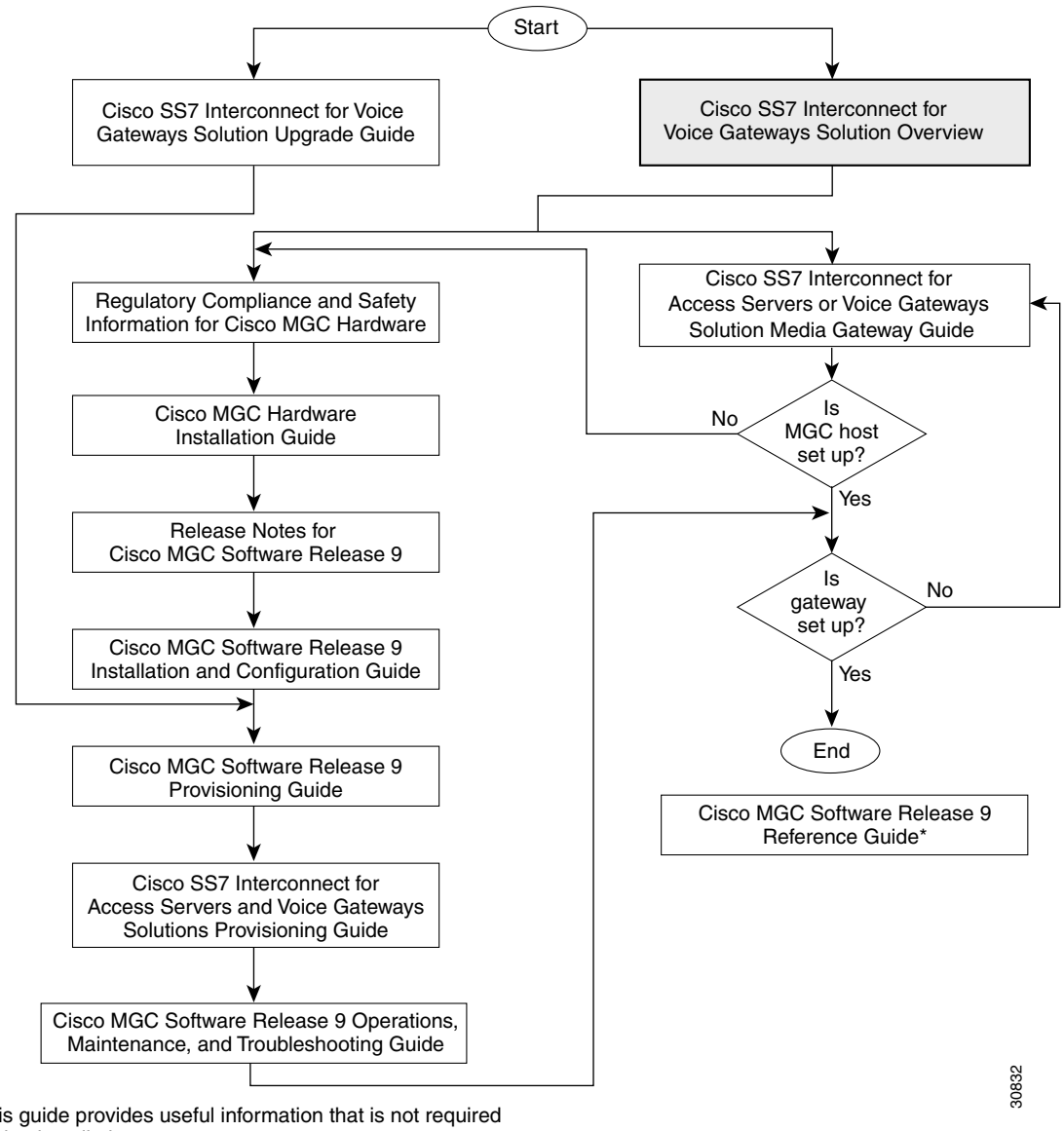
The major sections of this document are as follows

:

Chapters	Title	Description
Chapter 1	Introduction	Provides an introduction to the Cisco SS7 Interconnect for Voice Gateways Solution, describes architecture, benefits, features, and applications.
Chapter 2	Solution Configuration Options and Components	Provides information about configuration options and brief descriptions of components.
Chapter 3	Solution Operations	Describes unattended operations and manual control options.
Chapter 4	Implementation Overview	Provides high-level component configuration steps with pointers to detailed documents.
Appendix A	SS7 Technology	Provides a brief overview of the SS7 technology used in this guide.
Appendix B	Voice-over-IP	Provides a brief overview of the VoIP technology used in this guide.

Cisco SS7 Interconnect for Voice Gateways Solution Documentation Map

Refer to the following documentation map to navigate through the Cisco SS7 Interconnect for Voice Gateways Solution documentation suite. Note that the shaded box indicates the document you are currently reading.



* This guide provides useful information that is not required during installation.

Document Conventions

Command descriptions use the following conventions:

Table 1 SS7 Interconnect for Voice Gateways Overview Conventions

Convention	Description
boldface font	Commands and keywords.
italic font	Variables for which you supply values.
[ ]	Keywords or arguments that appear within square brackets are optional.
{x | y | z}	A choice of required keywords appears in braces separated by vertical bars. You must select one.
`screen font`	Examples of information displayed on the screen.
`boldface screen font`	Examples of information you must enter.
< >	Nonprinting characters, for example passwords, appear in angle brackets, in contexts where italics is unavailable.
[ ]	Default responses to system prompts appear in square brackets.

Note Means *reader take note*. Notes contain helpful suggestions or references to additional information and material.

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

Cisco SS7 Interconnect for Voice Gateways Solution Documentation Suite

Refer to the following documents for detailed hardware and software installation and configuration information about the Cisco SS7 Interconnect for Voice Gateways Solution:

- *Cisco SS7 Interconnect for Access Servers and Voice Gateways Solutions Provisioning Guide*
- *Cisco SS7 Interconnect for Access Servers and Voice Gateways Solutions Media Gateway Guide*
- *Cisco Media Gateway Controller Hardware Installation Guide*
- *Regulatory Compliance and Safety Information for Cisco Media Gateway Controller Hardware*
- *Cisco Media Gateway Controller Software Release 7 Installation and Configuration Guide*
- *Cisco Media Gateway Controller Software Release 7 Provisioning Guide*
- *Cisco Media Gateway Controller Software Release 7 Reference Guide*
- *Cisco Media Gateway Controller Software Release 7 Operations, Maintenance, and Troubleshooting Guide*

- *Release Notes for Cisco SS7 Interconnect for Voice Gateways Solution*
- *Release Notes for Cisco Media Gateway Controller Software Release 7*

Obtaining Documentation

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

World Wide Web

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

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

Documentation CD-ROM

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

Ordering Documentation

Cisco documentation is available in the following ways:

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

  http://www.cisco.com/cgi-bin/order/order_root.pl

- Registered Cisco.com users can order the Documentation CD-ROM through the online Subscription Store:

  http://www.cisco.com/go/subscription

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

Documentation Feedback

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

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

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

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

We appreciate your comments.

Obtaining Technical Assistance

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

Cisco.com

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

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

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

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

http://www.cisco.com

Technical Assistance Center

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

Contacting TAC by Using the Cisco TAC Website

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

http://www.cisco.com/tac

P3 and P4 level problems are defined as follows:

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

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

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

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

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

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

Contacting TAC by Telephone

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

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

P1 and P2 level problems are defined as follows:

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

CHAPTER 1

Introduction

This chapter introduces the Cisco SS7 Interconnect for Voice Gateways Solution and includes the following sections:

Overview

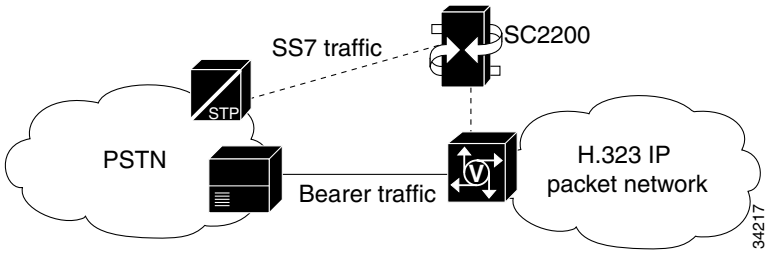
When you make calls using your telephone or PC with modem connection, you generally use the Public Switched Telephone Network (PSTN). You hear progress tones such as a dial tone or a busy tone that tell you your call is being processed. These are alerting tones that are produced by the PSTN. Alerting tones are used to communicate from the PSTN to users, and telecommunications computers, or "switches," communicate with each other through standards-based signaling. Signaling is the backbone for interconnection between carrier, cellular, and wireless networks. Signals are the medium that set up and tear down your calls.

A major breakthrough in signaling networks was to separate the signaling path from voice and data conversations. This is called "common channel interoffice signaling (CCS)." CCS, also known as out-of-band signaling, is a data network that overlays a carrier's switching network. Using CCS increases network intelligence, efficiency, automation, and functionality. CCS has evolved into a standard called Signaling System 7 (SS7), a protocol that lowered costs and increased network reliability even further. With SS7, all carriers are able to interoperate as a consistent and seamless network. Services such as global billing, wireless roaming, and 800 number calling rely on the SS7 protocol to exchange messages reliably.

The Cisco SS7 Interconnect for Voice Gateways Solution is a distributed system that provides SS7 connectivity for Voice-over-IP (VoIP) access gateways by using the Cisco Signaling Controller (also referred to as the Cisco SC2200 product) and the access gateways as a bridge from the H.323 IP network to the PSTN network. This solution interacts over the IP network with other Cisco H.323 VoIP access gateways. In addition, the Cisco SS7 Interconnect for Voice Gateways Solution can interoperate with H.323 endpoints, using non-SS7 signaling such as ISDN PRI and channelized T1.

Figure 1-1 illustrates where the Cisco SS7 Interconnect for Voice Gateways Solution is located when it is dropped into a PSTN to offload calls. By placing the solution as close to the ingress switch as possible, voice and data traffic ties up fewer PSTN resources. The direct connection of the Cisco SS7 Interconnect for Voice Gateways Solution to the SS7 network provides advantages such as faster call setups and teardowns, and SS7's look-ahead capabilities for rerouting to avoid downed network nodes and links.

Figure 1-1 With a Cisco SS7 Interconnect for Voice Gateways Solution



Cisco Signaling Controller Product Information

The Cisco signaling controller (Cisco SC2200) product is an application supported by the Cisco media gateway controller (Cisco MGC) product line that addresses the scalability of ISP dial modem traffic. The Cisco MGC is a powerful call control application that can be used to facilitate a wide variety of telecommunication services using data infrastructures. This new world architecture allows end users to realize the benefits of deploying a single network to address both data and voice applications.

Note Your Cisco SS7 Interconnect for Voice Gateways Solution documentation suite includes the Cisco MGC reference books.

Note Some product labels and packaging might use the term Cisco telephony controller. Any references to the Cisco telephony controller apply to the Cisco media gateway controller.

Understanding Terminology

The key terms used to describe the Cisco SS7 Interconnect for Voice Gateways Solution architecture are:

- Cisco SC2200—A hardware and software package that provides the signaling controller function. Typically this includes two SC hosts configured in a redundant manner for increased availability.
- SC host—A Sun host running signaling controller software.
- SC node—The combination of hardware (Sun servers and Cisco SLTs) and software that provides the signaling controller function and transports the signaling traffic between the SC hosts and the SS7 signaling network.
- SC zone—The combination of an SC node and the Cisco access gateways that are provided with signaling services.

Architecture

The Cisco SS7 Interconnect for Voice Gateways Solution architecture provides SS7 connectivity for voice gateways, by way of the SC host as a protocol translator, using ISDN Q.931 and SS7 as control protocols.

The solution consists of the following required components that are described in more detail in the "Cisco SS7 Interconnect for Voice Gateways Solution Components" section of this document.

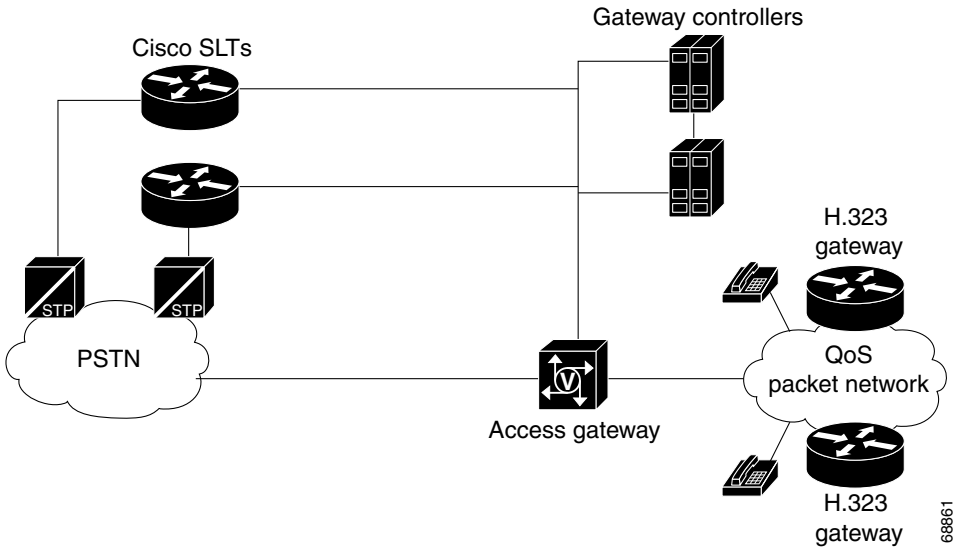
Table 1-1 Components for the Cisco SS7 Interconnect for Voice Gateways Solution

Component	Description
Cisco Signaling Controller Host	Cisco SC2200—operates as an SS7-to-ISDN protocol converter for the Cisco access gateways.
Cisco Signaling Link Terminal	Cisco SLT—used for physical SS7 link termination. • SLT 2611 • SLT 2651
Cisco Media Gateway	Used for bearer channel termination. • Cisco AS5300 • Cisco AS5350 • Cisco AS5400 • Cisco AS5800 • Cisco AS5850
Gatekeeper	Cisco 3640—manages other nodes in a VoIP network. (Optional.) **Note** This solution uses the Cisco 3640 gatekeeper, but supports any H.323 compliant gatekeeper used in your IP network.
LAN Switch	Cisco Catalyst Switch Family—a switch to extend Virtual Local Area Networks (VLANs) across platforms through backbone Fast Ethernet, Gigabit, or ATM connections. Connects multiple Cisco SLTs to the active and standby hosts within the SC node. Connects the media gateways with their controlling SC node. Connects the originating SC zone to the terminating SC node between SC zones. **Note** The switch is a customer premise equipment and is not provided with the Cisco signaling controller.
Cisco Media Gateway Controller Node Manager (CMNM)	Integrates the management interfaces and functionality of the Cisco MGC node components into a comprehensive human interface and data repository. (Optional.)

Table 1-1 Components for the Cisco SS7 Interconnect for Voice Gateways Solution

Component	Description
Cisco Voice Services Provisioning Tool (VSPT)	Provides a graphical user interface for the creation, modification, and execution of signaling connections, trunk groups, trunks, routes, and dial plans. (Optional.)
Cisco Internetwork Performance Monitor	Enables you to troubleshoot network-wide performance to diagnose congestion and latency problems. For more information, refer to the following URL: http://www.cisco.com/warp/public/cc/pd/wr2k/nemo/index.shtml
Cisco Resource Manager Essentials	A suite of Web-based applications offering network management solutions for Cisco switches, access servers, and routers. For more information, refer to the following URL: http://www.cisco.com/warp/public/cc/pd/wr2k/rsmn/index.shtml

Figure 1-2 Cisco SS7 Interconnect for Voice Gateways Solution Architecture



Benefits

Using the Cisco SS7 Interconnect for Voice Gateways Solution provides the following benefits:

- Provides wholesale dial services, dial-up Virtual Private Networks (VPNs), Internet access, and voice services, while interconnecting as a carrier.
- Provides network interface between the PSTN and the H.323 network.
- Addresses voice network congestion by using the SS7 interfaces to make features such as rerouting on overflow conditions and the use of IN functions possible, which further drives down operating costs.
- Replaces ISDN PRIs with bearer trunks and increase available bandwidth.
- Installs an SS7 POP in a new location without the added expense of a switch.

- Integrates the access gateways directly into the SS7 network, using the Cisco SS7 Interconnect for Voice Gateways Solution, and thus remove the need for two switch ports on the PSTN circuit switch for each NAS port installed.
- Increases the signaling channel to bearer channel ratios, thus decreasing the number of signaling channels needed and the overall complexity of the system or network.
- Provides economical reliability of SS7 link termination by using channelized T1/E1/T3 software on the Cisco SLT.
- Transparently passes individual and uncompressed T1/E1/T3 channels between T1/E1/T3 ports using Drop and Insert interfaces.
- Provides enhanced scalability of PSTN and packet network interconnectivity.
- Provides enhanced usability of the Cisco SC2200 system utilities.

Features

Table 1-2 briefly lists features that are provided with your Cisco SS7 Interconnect for Voice Gateways Solution. For an overview of scalability and performance, system redundancy, management, and software requirements, see subsequent sections of this document.

Table 1-2 Features for the Cisco SS7 Interconnect for Voice Gateways Solution

Feature	Purpose
Directly connects access gateways to PSTN in a peer-to-peer interconnect	• Reduces network costs • Interconnects with more favorable tariffs and rates
Supports Cisco H.323 access gateways and gatekeepers	Provides SS7 connectivity for intelligent H.323 endpoints: • Offers long-distance and international low-rate telephony services • Uses packet telephony technology for cost-effective offloading of voice traffic from congested PSTN networks
Supports co-located and distributed access gateways	• Cost savings; scalable and flexible
Terminates and originates switching-system functions	• Enables new services • Fast time to market • Dial-out and dial-in • Meets interconnect requirements
Worldwide protocol support using Cisco Message Definition Language (MDL).	• Is certified worldwide • Fast time to market
Provides software upgrade of: • Cisco IOS • Signaling controller and Sun OS software • Cisco Signaling Link Terminal	• Protects Cisco investments • Provides low cost of ownership • Is part of a complete solution with Cisco IOS software

Table 1-2 Features for the Cisco SS7 Interconnect for Voice Gateways Solution (continued)

Feature	Purpose
Provides a reliable IP link between signaling controllers and access gateways with Redundant Link Manager (RLM)	No single point of failure in connection between access gateways and signaling controllers
• RADIUS or TACACS+ AAA functions, including authentication based on calling or called number • Provides call detail records for PSTN billing • RADIUS Proxy (GRS)	Meet PSTN requirements to create new service opportunities
Provides facility associated signaling through the Cisco SLTs	• Grooms the bearer channels and then delivers, or hairpins, them to the access gateway • Backhauls MTP-3 to the Cisco SC2200 over Reliable User Data Protocol/Internet Protocol (RUDP/IP)
Fault-tolerant platform	• Provides no more than 6 seconds of downtime per year
Continuous service platform	• Established calls are maintained upon failover
Sun OS 2.6.1	• Y2K compliant • Open computing platform
Cisco MGC Manager (CMM)	• Full SNMP configuration

Scalability and Performance

The Cisco SS7 Interconnect for Voice Gateways Solution includes the following scalability and performance features:

- Support for up to 100,000 DS-0 ports
- Ability to process 80 calls per second with 100,000 simultaneous calls of 20 minute call hold time
- Support for up to 180,000 busy hour call attempts
- Support for 250+ destination point codes (DPCs)
- Support for 6 originating point codes (OPCs)
- Support for quasi-associated or fully associated signaling
- Complete continuity check (two-wire and four-wire)
- Compliant with NEBS Level 3 standards

System Redundancy

For maximum reliability and resilience, Cisco recommends the following options:

- Deploying the Cisco SS7 Interconnect for Voice Gateways Solution continuous service configuration at your site. The continuous service configuration consists of an active server and a standby server, linked by a heartbeat function. All configuration changes made to the active server are replicated on the standby server.
- Using a minimum of two LAN switches from the Cisco Catalyst switch family that support:
  - Inter-Switch Link (ISL) trunking protocol configured between the two switches.
  - One route-switch module (RSM), which routes traffic between the VLANs when necessary.
- Using a minimum of two links per linkset if signaling links are connected to the Cisco signaling controllers. The links should be split across separate T1/E1 interface cards on the LAN switches, SC hosts, and Cisco SLTs.

Signaling Controller Management

Table 1-3 provides an overview of the management components of the signaling controller.

Table 1-3 Management Components of the Signaling Controller

Management Component	Description
Configuration Management	Dial Provisioning Plan (DPP) is used to format the dial plan and routing data for deployment on the signaling controller. Dial plan and routing data is defined in a flat file, and this information is parsed by the DPP to generate the configuration files for deployment on the signaling controller.
Fault Management	The signaling controller supports a comprehensive set of alarms: • Configuration • Resource • Operating system • I/O card • Signaling channel failure • Line interface loss of signal You can customize the severity of alarm and thresholds to match your carrier's severity level definitions. You can also configure the system to generate real-time alarms to local or remote terminals. All alarms are written to a log file in an uncompressed format for easy retrieval.

Table 1-3 Management Components of the Signaling Controller (continued)

Management Component	Description
Performance Management	You can get a variety of usage statistics from the signaling controller. The data is recorded real-time and is written to a file. You can specify the statistics to be collected and the time intervals for collection and writing to the file. Each performance measurement record includes: • Start time • Duration • Measured value • Category • Element measured
Accounting Management	Every call that passes through the signaling controller produces call detail information, which includes: • CLI pretranslated • CLI posttranslated • Dialed number pretranslated • Dialed number posttranslated • Start, seizure, supervision, and disconnect time stamps • Circuit path information Call detail records are written to a spool file that is automatically closed at defined intervals or when the file exceeds a specified size. You can also specify when to retrieve or send closed files to processing systems.

Access Gateway Management

The Cisco IOS software installed on the access gateways provides an array of network management components (described in Table 1-4) designed to meet the needs of today's large, complex networks.

These management features do the following:

- Reduce network bandwidth and processing overhead
- Offload management servers
- Conserve resources
- Ease system configuration tasks

Cisco's integrated management simplifies administrative procedures and shortens the time required to diagnose and fix geographically dispersed networks with a small, centrally located staff of experts. Configuration services reduce the cost of installing, upgrading, and reconfiguring network equipment.

Table 1-4 Network Management Components

Management Component	Description
SNMP and RMON Support	Access gateways are fully manageable by using the Simple Network Management Protocol (SNMP) and imbedded Remote Monitoring (RMON) capabilities: • SNMP provides for the collection of information about each controller and interface, which can be polled through any SNMP-compatible network management system. • RMON acts as a remote protocol analyzer and LAN probe. By using the Alarm RMON group, you can set a threshold on any integer-valued Management Information Base (MIB) variable. When the threshold is crossed, an event, defined in the Event RMON group, is triggered. With these capabilities, the system can detect and analyze overloaded conditions and congestion in real time.
Network Management Systems	The access gateways both support CLI and CiscoView graphical user interface (GUI) for comprehensive, flexible network management. CiscoView provides dynamic status, statistics, and comprehensive configuration information for Cisco switches, routers, access gateways, Cisco SLTs, concentrators, and adapters. It displays a graphical view of Cisco devices, provides configuring and monitoring functions, and offers basic troubleshooting.
Modem Management	Cisco offers two types of modems: basic and managed. Managed modems offer superior reporting and statistics in the CiscoView application, including troubleshooting and monitoring modem connections on individual or groups of modems, while calls are in progress. You can manage modems using the same tools used to manage the rest of the network. In addition, managed modems provide an out-of-band management feature that allows you to reduce problem detection and resolution time from a remote site. Through out-of-band management, you can view real-time information (for current or previous calls) such as modem modulation scheme, modem protocol, modem EIA/TIA-232 signal states, modem transmit and receive states, and analog signal-to-noise ratio.

Cisco Signaling Link Terminal Management

The Session Manager software, running on the Cisco SLT, manages the communication sessions between two SC hosts.

The session manager:

- Maintains separate communication sessions with each signaling controller in the pair
- Uses RUDP to communicate between the Cisco SLT and the signaling controller
- In a continuous service configuration, handles additional traffic in the event of a single Cisco SLT failure, with no impact to call processing

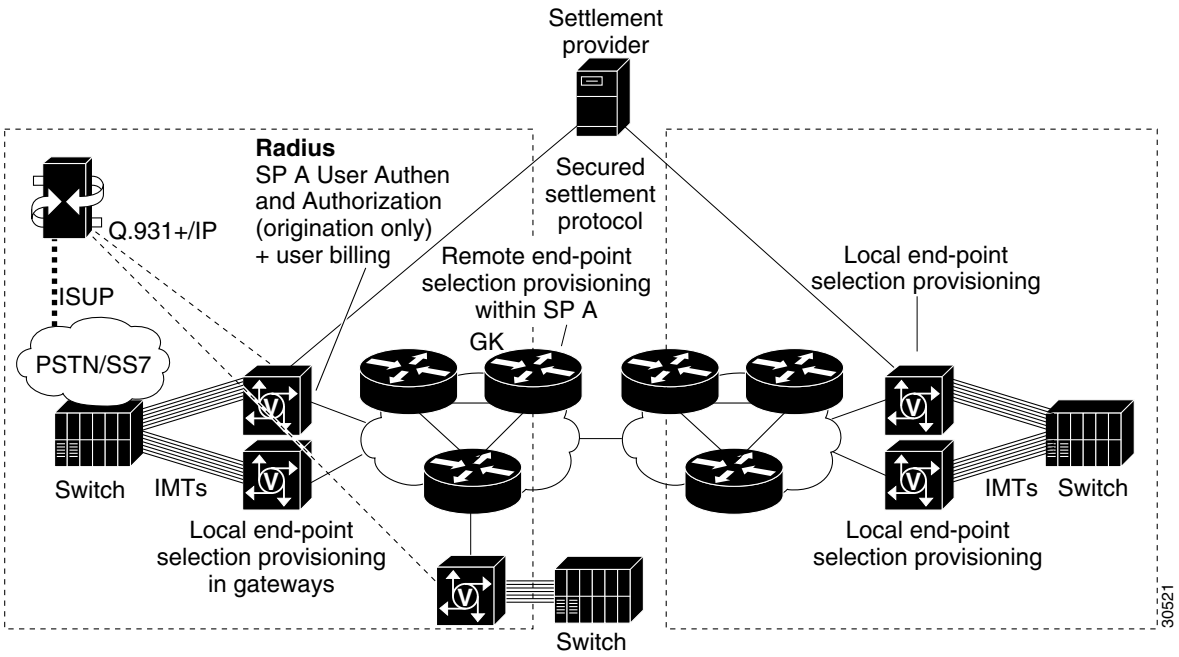
Applications

The Cisco SS7 Interconnect for Voice Gateways Solution preserves full capabilities on the IP side, including existing H.323 access gateway functionality, interoperability with H.323 gatekeepers, two stage dialing, mixed gateway environment, and PSTN voice and fax traffic offload. This solution targets the following key applications that support phone to phone, PC to phone, and fax relay packet telephony services:

- Two-Stage-Dial Toll Bypass
- PSTN Voice and Fax Traffic Offload
- Packet Telephony and Data Wholesale Services

Settlement providers require services such as two-stage dialing, international toll bypass, and open settlements, as illustrated in Figure 1-3.

Figure 1-3 A Typical Settlement Provider Application



Two-Stage-Dial Toll Bypass

This application enables the service provider to leverage its WAN infrastructure and offer long-distance toll bypass services. Each customer is assigned an account number and a personal identification number (PIN). The user dials a local or a 1-800 Internet Telephony Service Provider (ITSP) number and is connected to the local VoIP point of presence.

In Figure 1-3, the first leg of the call is terminated by the access gateway through the ISUP to Q.931+/IP translation. The user is prompted by the interactive voice response (IVR) to input account and PIN numbers, and (following an authentication by the RADIUS server) then a secondary dial tone allows the desired phone number to be entered. Also, the RADIUS authentication can be accomplished based on the combination of calling number ID (ANI) and called number (DNIS).

For fax services, the PIN number is automatically dialed by the redialer that is attached to the fax machine. An E.164 destination phone number, dialed by the user, is mapped by the local-zone gatekeeper to an IP address of a remote-zone gatekeeper. The remote-zone gatekeeper selects an access gateway to terminate the call. During the call setup, end-to-end ISUP signaling transparency is supported. After the call setup is complete, the voice is encoded by the access gateway using standard algorithms (including G.711, G.729, G.729a, and G.723.1), encapsulated in Real-Time Transport Protocol (RTP) packets, and then routed over the WAN to the remote access gateway that decodes the voice and delivers it to the receiver.

PSTN Voice and Fax Traffic Offload

This application offloads PSTN traffic from congested PSTN networks. The offloaded traffic is then forwarded to a tandem switch connected in a peer-to-peer configuration to the Cisco SS7 Interconnect for Voice Gateways Solution through access gateways. The configuration uses Direct Inward Dialing (DID) functionality, and no ANI or CDR billing is required.

Packet Telephony and Data Wholesale Services

This application enables the wholesale service provider to extend services to a specific geographical area. Again, voice and fax traffic is offloaded from PSTN onto data networks, as well as support scalable routing and Quality of Service (QoS), across data networks, to effectively route the calls to their final destination. Routing and authorization between multiple service carriers, and real-time selection of a cost-effective service provider and reciprocal billing arrangements are required. Resource pooling is required for data, but not for voice.

The Open Settlement Protocol (OSP) is a communications protocol between H.323 equipment and back-end services, such as authorization, route determination, and call detail record (CDR) collection and settlement. With OSP, interdomain CDR records are forwarded to the settlement system, processed, and then transmitted as settled records to billing system platforms. The access gateways in your Cisco SS7 Interconnect for Voice Gateways Solution generate intradomain records and are accessed by any accounting and billing system based on RADIUS.

CHAPTER 2

Solution Configuration Options and Components

This chapter briefly describes the various Cisco SS7 Interconnect for Voice Gateways Solution configuration options and the required and optional components:

Cisco SS7 Interconnect for Voice Gateways Solution Configurations

The Cisco SS7 Interconnect for Voice Gateways Solution provides the following configuration options:

- Simplex and Redundancy Options
- Signaling Network Connection Options
- Control Signaling Network Options

Simplex and Redundancy Options

You can deploy the Cisco SS7 Interconnect for Voice Gateways Solution in one of the following configurations:

- Simplex Configuration
- Continuous Service Configuration

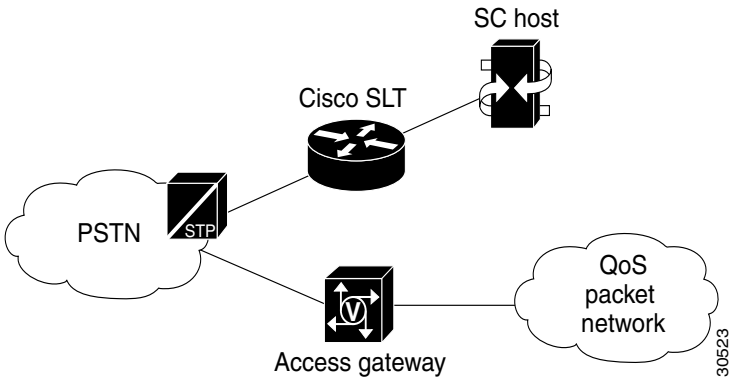
Simplex Configuration

A simplex configuration is an SC zone that consists of a single SC host operating with one or more Cisco SLTs. The SC application is run on the SC host and the SS7 signaling links are terminated on the Cisco SLT. An IP control LAN is used to interconnect the host server with the Cisco SLTs. One or more access gateways are required for bearer channel termination. See Figure 2-1.

Quality of Service (QoS) packet network in Figure 2-1 refers to a packet network in which both bandwidth control and latency control are achieved for the particular application.

Note Simplex configurations provide no fault tolerance and are typically used for solution testing or validation or noncritical installations. If the host fails, calls are dropped, and service is discontinued.

Figure 2-1 Simplex Configuration Example

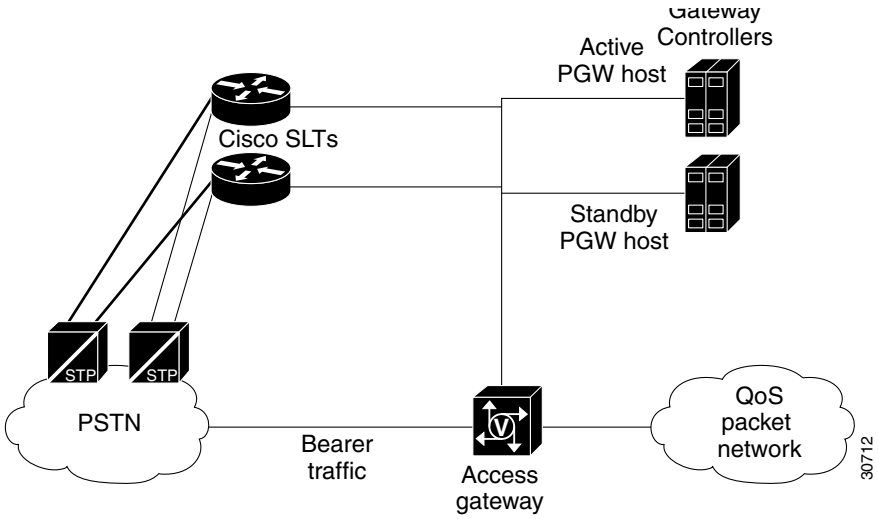


Continuous Service Configuration

A continuous service configuration is an SC zone that consists of a pair of SC hosts running in an active (primary) and standby (secondary) mode, operating with one or more access gateways and one or more Cisco SLTs. An error-checking function runs continuously between the two SC hosts, monitoring the primary SC host. When the function detects an error condition on the primary SC host, responsibility for call processing is switched to the secondary SC host. The secondary SC host now becomes the active SC host; call preservation is maintained.

Figure 2-2 shows an example of a continuous service configuration with redundant signaling links terminating on a pair of Cisco SLTs with bearer traffic terminating on the access gateway.

Figure 2-2 Continuous Service Configuration Example



Signaling Network Connection Options

The Cisco SS7 Interconnect for Voice Gateways Solution performs functions to exchange telephone control messages between the following components that support the end user's signaling network connection:

- Cisco Signaling Controller—Provides a signaling protocol conversion and network Q.931 call control to communicate with the access gateways. One signaling controller might provide signaling and call-processing services for multiple access gateways in geographically distributed locations, over redundant IP links used for ISDN signaling.
- Cisco SLT—Handles the incoming and outgoing SS7 messages (MTP layer 1 and 2) from the A-links (access links) connected to Signal Transfer Points (STPs) or F-links connected to Service Switching Points (SSPs). Also, when used in Drop-and-Insert mode, the Cisco SLT grooms off the terminating signaling link from F-links (fully associated links) and then hairpins the bearer channels (ISUP) to the access gateway.
- Cisco Access Gateway—Provides termination for PSTN trunks. An access gateway functions as a server to the SS7 bearer links. The access gateway has at least two IP network interfaces: one to carry IP packet data onto one or more of the Internet Service Provider's (ISP's) backbones and another to connect to the ISP's secure management, signaling, and Q.931 control network.

Your Cisco SS7 Interconnect for Voice Gateways Solution can be deployed in three ways, as described in "Simplex and Redundancy Options" section on page 2-1, with the following SS7 signaling network connections.

Note Type of connection would depend on your specific network requirements.

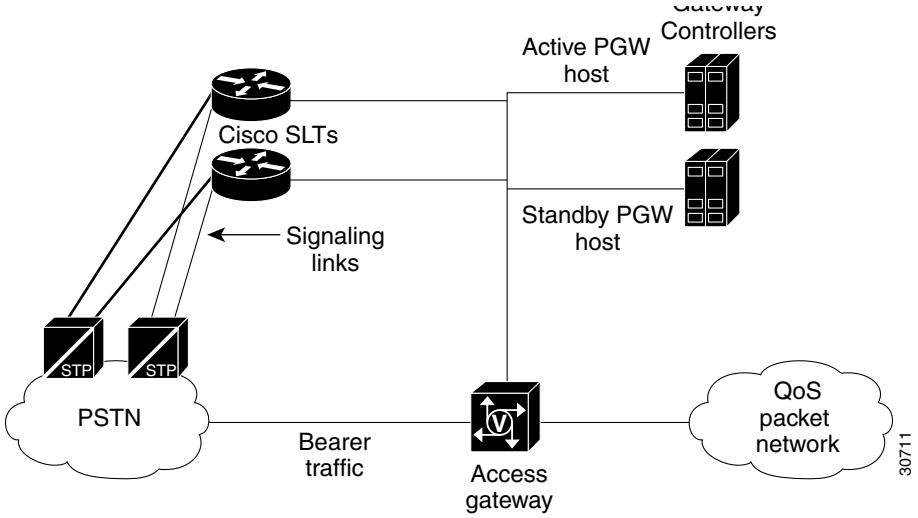
- A-Link with Cisco SLT
- F-Link with Cisco SLT
- A-Link or F-Link with Cisco SLT (Drop-and-Insert)

A-Link with Cisco SLT

An A-link with Cisco SLT signaling connection is an access link from the PSTN Signal Transfer Point (STP) connected to the Cisco SLT of the SC node, through EIA/TIA-449, EIA/TIA-530, V.35, and T1/E1 interfaces. This option can be used with simplex and continuous service host configurations. Each interface supports a single signaling channel.

In the A-link SLT signaling connection, the Cisco SLT processes the two lowest-level SS7 signaling protocols, MTP1 and MTP2. The upper layer protocols are then forwarded to the SC host over the control signaling network. Each Cisco SLT supports two signaling network connections. Multiple Cisco SLTs can be used to support additional signaling channels or provide redundant signal paths between the signaling network and the control signaling network, as illustrated in Figure 2-3.

Figure 2-3 A-Link SLT Signaling Configuration



F-Link with Cisco SLT

An F-link with Cisco SLT signaling connection is a fully associated link from the SS7 network to the Cisco SLT of the SC node. F-links connect the SC host directly to a Service Switching Point (SSP) or a Service Control Point (SCP) in the SS7 network; they do not make an intermediate connection through STPs.

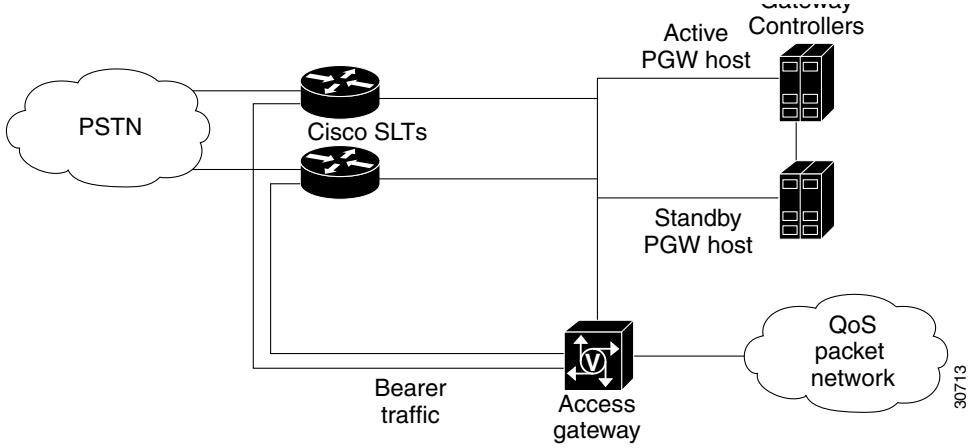
The F-link SLT signaling configuration supports EIA/TIA-449, EIA/TIA-530, V.35, and T1/E1 interfaces that are installed in the Cisco SLT. The F-link SLT configuration can be used with simplex and continuous service SC host configurations. Each interface supports a single DS0 signaling channel.

A-Link or F-Link with Cisco SLT (Drop-and-Insert)

An A-link or F-link with Cisco SLT (Drop-and-Insert) signaling connection is similar, respectively, to an A-link or F-link SLT signaling connection. Fully associated links directly connect an SSP or SCP to the Cisco SLT. The difference is that the A-link and F-link Drop-and-Insert configurations support a single DS0 signaling channel per link and additional bearer traffic channels up to the capacity of the T1 or E1 link as shown in Figure 2-4.

Note The F-link Drop-and-Insert technique is also known as time-division multiplexing (TDM) cross-connect.

Figure 2-4 F-Link Drop-and-Insert Configuration



The F-link Drop-and-Insert signaling configuration supports T1 and E1 interfaces using signaling interface cards installed in the Cisco SLT. The Drop-and-Insert cards are special two-port cards designed for this application. Signal and bearer traffic enter one port together, then the Cisco SLT separates the bearer traffic and routes it out the second port.

The F-link Drop-and-Insert configuration can be used with simplex and continuous service host configurations. Each interface card supports a single DS0 signaling channel.

Control Signaling Network Options

Designing your network to handle control signaling is a complex and sophisticated task beyond the scope of this document. This section briefly describes what control signaling network options are available and some network engineering guidelines to consider.

Customer-Provided Equipment

Your control network consists of a number of hubs, switches, or routers configured together to support the number of ports in your point of presence (POP), the traffic characteristics of incoming calls, the geographic location of the Cisco SS7 Interconnect for Voice Gateways Solution components, and the level of redundancy that you require. Other factors to consider are:

- Design of the network (topology and hardware components)
- Security (physical, packet encryption, packet filtering)
- Quality of service (delay, bandwidth, throughput, queuing techniques)
- Traffic segregation (access lists and route filters)
- Configuration of the components (RLM with the required SC host and access gateway/Cisco SLT redundancy, and timers)

Control traffic (signaling) should be segregated from the bearer data IP traffic (towards the internet/intranet) onto a different network. This optimizes control traffic latency and provides added security. Redundancy in your control network can be provided by duplicating your Cisco SS7 Interconnect for Voice Gateways Solution components. In the event that the control network fails or connectivity to it fails, the data network is used for signaling.

In the simplest case, your Cisco SS7 Interconnect for Voice Gateways Solution components are co-located and a pair of LAN switches serve as your control network. However, it is also possible that Cisco SLTs, and access gateways, are geographically separate from the SC hosts, requiring a control network with WAN links and separate routers to provide the WAN connection.

IP Connectivity with LAN

Figure 2-2 shows a sample continuous configuration with a mated Cisco SLT pair (for redundancy) on the control signaling network. Redundant signaling controllers support two or four Fast Ethernet connections each.

In this continuous configuration example, the control network functions are:

- Checkpointing traffic (RUDP/UDP/IP)
- Heartbeat (UDP; 50 bytes/second)
- SNMP management of components (configurable to either network)
- SC host/access gateway signaling and communications (Q.931+/Q921/UDP/IP-RLM)
- SC host/Cisco SLT signaling and communications (MTP-3+ISUP/SM/RUPD/UDP/IP)

The QoS packet network functions are:

- PSTN traffic over IP from and toward the Internet/Intranet
- H.323 access gateway traffic
- Access gateway/AAA (Radius/TACACS+server traffic)

IP Control Network Combinations

The following IP control network combinations are recommended:

- One single subnet for all traffic.
- Two redundant subnets: one dedicated to control traffic and the other for user data traffic and as alternative path for the control traffic.
- Four redundant subnets: two redundant subnets for Cisco SLT/SC host traffic; two redundant subnets for access gateway/SC host traffic.

  Note One of these subnet pairs must also run user data traffic.

- Any combination of the above with VLANs configured in shared switches.

Note The subnet mentioned in your IP control network can be a dedicated hub or switch running at 10 or 100 Mbps (10 Mbps for SLTs) or a VLAN configured in a switch sharing backplane bandwidth with other VLANs.

Engineering Considerations

When engineering your network, you must consider the following issues:

- There should be no packet loss, and the packets should not be received out of order between the signaling controller and the access gateways. This could impact the performance of the Cisco SS7 Interconnect for Voice Gateways Solution, and the call setup time might become unacceptable.
- Do not enable load balancing in the control network. If you must use load balancing, you must also enable destination-based load balancing. In this case, use Cisco Express Forwarding (CEF) if available. If you do not use CEF, load balancing could cause out-of-sequence delivery when the cache ages out.
- If you are using weighted fair queuing (WFQ) or any other type of queuing feature, make sure that all signaling packets from the access gateways to the signaling controller (and vice versa) show up in the same queues. Fancy Queuing is not recommended in the control network unless absolutely necessary.
- If you are using dynamic routing protocols in the control network, out-of-sequence delivery could occur on a change of adjacency or topology. This should not be a normal occurrence in a stable network.

Cisco SS7 Interconnect for Voice Gateways Solution Components

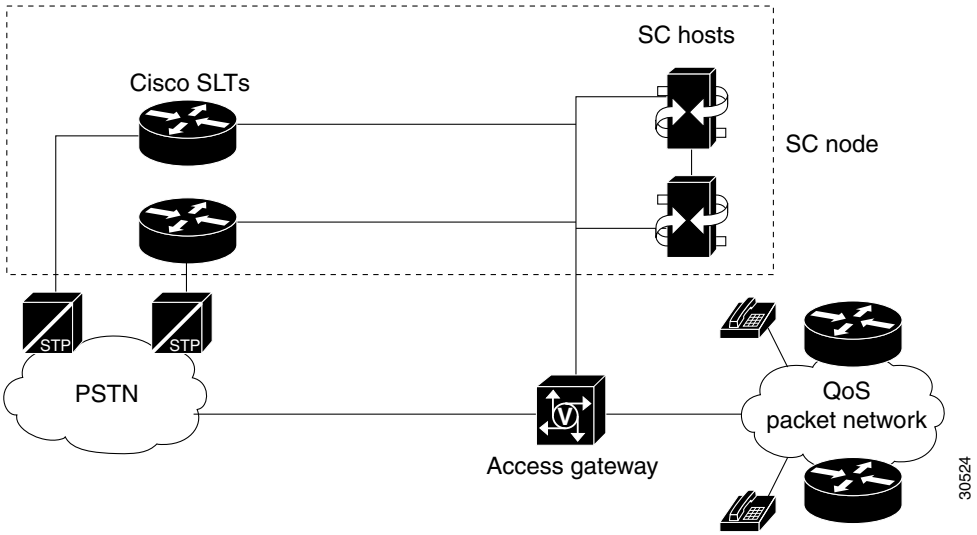
The Cisco SS7 Interconnect for Voice Gateways Solution contains the following components:

- SC Node Products
- Access Gateways
- LAN Switches (Optional)

Figure 2-5 displays the components of the Cisco SS7 Interconnect for Voice Gateways Solution.

See the "Overview" appendix for information about how the solution components operate within the SS7 hierarchy.

Figure 2-5 Cisco SS7 Interconnect for Voice Gateways Solution Components



SC Node Products

The SC node is the combination of hardware and software that provides the signaling controller function and transports the signaling traffic between the SC hosts and the SS7 signaling network. The SC node in the Cisco SS7 Interconnect for Voice Gateways Solution consists of one or more SC hosts, one or more Cisco SLTs, the signaling controller software, and ancillary equipment.

SC Host

An SC host is a Sun hardware platform running signaling controller software.

Table 2-1 lists supported SC hosts for the Cisco SC2200 product.

Table 2-1 Supported SC Hosts

SC Host	Description
Sun Netra t 112x	The Sun Netra t 112x is a general-purpose Sun Ultra SPARC server. The Sun Netra t 112x is rack-mountable and is NEBS and ETSI compliant.
Sun Netra t 140x	The Sun Netra t 140x is a fault-tolerant, dual modular, redundant architecture. Additional lockstep operations give this host the ability to isolate and recover from hardware failure.

SC Host Features

The primary functions of the signaling controller is performing protocol conversion and call screening. The signaling controller is responsible for:

- Interworking multiple-user protocols
- Translating dialed digit information into data address information A-number and B-number analysis
- Issuing control commands to the Transport layer to create, modify, or delete a call session now is
- Generating comprehensive CDR on a call-by-call basis
- Providing element management information and statistics
- Providing comprehensive signaling debugging capabilities

Table 2-2 lists the features for the SC hosts.

Table 2-2 SC Host Features

Feature	Support for ...
Call performance per signaling controller (simplex configuration with 20 minute call hold time)	• 80 call-per-second rate with 100,000 simultaneous calls on VSC Sun Netra t 140x platform, or, • 45 call-per-second rate with 45,000 simultaneous calls on VSC Sun Netra t 1120 platform.
Call performance per signaling controller (continuous service configuration)	• 80 call-per-second rate with 100,000 simultaneous calls on VSC Sun Netra t 140x platform, or, • 45 call-per-second rate with 45,000 simultaneous calls on VSC Sun Netra t 1120 platform.
Performance	• Provisioning from MML or from an SNMP manager • Dynamic reconfiguration of point codes, linksets, trunk groups, and trunks • MML commands and responses • Application-level checking of call states and circuit states
Signaling protocols	• SS7 with MTP2 configured on the Cisco SLT • Support for national protocols of many countries
Scaling of point codes	250+ DPCs and 6 OPCs
Network management interfaces	IP
Faults and alarms management	SNMP traps
Millisecond Timestamp	Millisecond time stamps on log records of diagnostic messages, set and clear alarm messages (sets and clears), alarm messages recorded by the Data Dumper, and alarm messages in the responses for the MML commands **rtrv-alms** and **rtrv-alms:CONT**.

Table 2-2 SC Host Features (continued)

Feature	Support for ...
Logging enhancements for Release 1.1	Improved system logging efficiency and your ability to diagnose problems. The logging utility is enhanced in the following areas: • Enhanced log format: consistent, text-based message logs • Improved system efficiency: dynamic and non-service interrupting filtering capabilities for specific logging. • Improved user efficiency: inter-workability with other tools, such as grep utility, and improved log reliability.
Configuration management	• Call Controller Manager (CCM), a TCL/tk graphic user interface (GUI) that uses Simple Network Management Protocol (SNMP) commands to provision the Cisco media gateway controller (MGC). **Note** Call Controller Manager (CCM) is also referred to as Telephony Controller Manager (TCM) in earlier releases of this solution. • Man-Machine Language, a command-line interface to the MGC
Accounting	CDR (CSV format) support for international carrier requirements
Resource management	• Keeps track of circuit IDs for assigning calls on access gateway ports • Manages adds, moves, and changes of access gateway resources
Performance measurements and statistics	Supports carrier requirements
Security	Structured system of passwords
Operating system	Sun Solaris 2.6.x
Dial Plan Provisioning Enhancements	Enable you to input a shortest digit sequence to the Cisco SC2200 number analysis table to define a range of digit strings for the same digit analysis treatment. For example, for North America Numbering Plan (NANP) dial plans, the shortest digit sequence to identify the range of digit strings from 1 703-484-3000 through 1 703-484-3999 for the same digit analysis treatment would be 1 703-484-3 in the number analysis tables.
MML-control of call processing resources	Provide a MML command interface to allow or reject any new calls.
Route List Display	Display the symbolic name of a route list in the Telephony Controller Manager (TCM).

Table 2-2 SC Host Features (continued)

Feature	Support for ...
Configuration Upload/Download	Provide new configuration management capabilities using both the SNMP and MML interfaces to upload or download all the non-static configuration information.
MML Names in Log	Display component IDs in the terms of MML names in system logs.
Bearer Channel Level Tracing	Provide a call tracing capability using the MML interface to generate machine-readable traces to be used by Call Trace Viewer (CTV) applications.
Viewer Tools	Provide the following new viewing aids for system-generated data files: • Call Trace Viewer: A tool to display the specified call trace file. • CDR Viewer: A GUI-based tool to retrieve and display the specified CDR file or files. • Log Viewer: A GUI-based tool to retrieve and display the specified Cisco SC2200 log file or files. • Route Verification Viewer: A tool to display the summary of route translation by simulating the specified call through the active dialplan.
Memory Reduction	Provide a per-call, post-answer memory reduction mechanism to accommodate 100,000 simultaneous calls on Cisco SC2200 with the Netra ft 1800 SC host. **Caution** The Memory Reduction mechanism may degrade the calls-per-second (CPS) rate. If CPS degrades by more than 5 percent, Cisco recommends that you disable this feature. Cisco also recommends that you never allow CPS to degrade by more than 20 percent.

Cisco SLT

The Cisco SLT handles the incoming and outgoing SS7 messages (MTP layer 1 and 2) that arrive from the PSTN Signal Transfer Points (STPs) or Service Switching Points (SSPs). When used in the proper configurations, the Cisco SLTs improve fault tolerance by providing for multiple communications paths between the SS7 signaling network and multiple SC hosts.

Cisco SLT Features

Table 2-3 lists Cisco SLT features.

Table 2-3 Cisco SLT Features

Feature	Support for...
SS7 link termination on a high-availability platform	SS7 network access and interconnection requires a high degree of reliability in the signaling links and associated equipment. The Cisco SLT provides the reliability of a dedicated signaling link termination device and maximizes the availability of the SS7 signaling links.
Distributed SS7 MTP processing	Processor-intensive parts of the SS7 Message Transfer Part (levels1 and 2) are offloaded from the signaling controller to the Cisco SLT. This distributed MTP model allows the signaling controller to better utilize its resources to provide optimal call control.
Call control	Signaling backhaul provides a means for integrating the signaling link terminals into a virtual switch with the call control intelligence centralized in the signaling controller system.
Standard physical interfaces	Interconnection with SS7 network elements is supported using the most popular SS7 physical interface standards: T1, E1, T3, V.35, EIA/TIA-449, and EIA/TIA-530.
Drop-and-Insert	Cisco T1/E1 Multiflex Voice/WAN interface cards support Drop-and-Insert (also called TDM Cross-Connect), which allows individual T1/E1/T3 channels to be transparently passed, uncompressed, between T1/E1/T3 ports. This feature enables direct termination of SS7 F-links in T1/E1/T3 carriers, while the remaining bearer channels are hairpinned back to a gateway device for processing.

Cisco Media Gateway Controller Node Manager

CMNM provides the element-specific management features for the SC node. It blends the management framework features of the Cisco Element Management Framework (CEMF) with the individual interfaces and object structures of each managed element to produce an integrated management application. Table 2-4 lists the features of CMNM.

Table 2-4 Cisco Media Gateway Controller Node Manager Features

Feature	Benefit
Performance monitoring	Collects performance information from the individual components of the SC node, allowing you to monitor the health and performance of the network.
Fault management	Provides fault management of the SC node, including the SC host, the Cisco SLT, and the optional LAN switch.

Table 2-4 Cisco Media Gateway Controller Node Manager Features (continued)

Feature	Benefit
Security	• Supports role-based access to management functions. The administrator defines user groups and assigns users to these groups. • Supports control of administrative state variables for SC node resources.
Troubleshooting	Provides the following for diagnostic and troubleshooting information: • CDR Viewer • Log Viewer • Trace Viewer • Translation Verification Viewer

Cisco Voice Services Provisioning Tool

The Cisco VSPT provides a graphical user interface (GUI) for the creation, modification, and execution of signaling connections, trunk groups, trunks, routes, and dial plans. It also allows users to import existing configurations for modification and then download the modified configurations to the same or different devices. To simplify operator tasks, such as trunk group provisioning, the Cisco VSPT employs a series of wizard-style templates combined with a user interface tailored for provisioning. Cisco VSPT automatically generates the Man Machine Language (MML) or command-line interface (CLI) scripts used to configure the network elements. Cisco VSPT may be used to bulk-create the initial network provisioning information for a newly installed node, creating iterative entries from a single operation action. It can also provide incremental provisioning of individual call parameters, simplifying the provisioning of large live networks.

Access Gateways

The access gateway terminates the PSTN trunks, also referred to as bearer channels, that carry the call traffic. The PSTN trunks are T1/E1/T3 PRI interfaces. In addition, the access gateway performs call control (including originating and terminating call processing/signaling).

Table 2-5 lists the features for the Cisco AS5*x*00.

Table 2-5 Cisco AS5x00 Features

Feature	Support for...
Continuity testing	Automated diagnostic procedure
Redundant Link Manager	Virtual link management

LAN Switches (Optional)

The control signaling network for the Cisco SS7 Interconnect for Voice Gateways Solution often consists of a LAN switch and the cabling required to interconnect the solution components in an SC zone. This solution supports a LAN switch from the Cisco Catalyst switch family. This switch can extend VLANs across platforms through backbone Fast Ethernet, Gigabit, or ATM connections, when necessary.

Note The Catalyst LAN switch is not provided with the Cisco SC2200 product.

CHAPTER 3

Solution Operations

This chapter provides a brief overview of unattended operations and manual control options available on your Cisco SS7 Interconnect for Voice Gateways Solution. It includes the following sections:

Unattended Operation

The following operations are described in this section:

Understanding System Redundancy

The Cisco SS7 Interconnect for Voice Gateways Solution uses two SC hosts with software-based checkpointing and heartbeat to facilitate redundancy. The call-processing application is active on only one SC host platform at a time and switches to the standby platform under failure conditions. See the "Understanding Automatic Switchover" section.

The Session Manager software on the Cisco SLT manages the communication sessions with the SC hosts. When Cisco SLTs are used with a redundant pair of SC hosts, the Session Manager maintains separate communication sessions with each SC host in the pair. The session between the Cisco SLT and the active SC host transports the SS7 traffic, while the session between the Cisco SLT and the standby SC host provides backup. Upon SC host switchover, the Session Manager on the Cisco SLT must be instructed by the now active (formerly standby) SC to switch traffic to the now active SC host. On switchover, all calls answered in progress are preserved.

Note Full system redundancy is available with continuous service configurations.

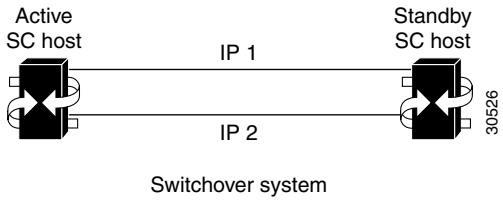
Understanding Automatic Switchover

The Cisco SS7 Interconnect for Voice Gateways Solution offers the continuous service configuration to protect your system against failures and downtime. A feature enhancement to RLM (Version 2) provides redundancy at the link and signaling controller level for added switchover. When each RLM group has multiple signaling controllers associated with a NAS, a signaling controller priority and link priority are examined by the RLM client (RLM software on the NAS) during switchover, ensuring improved control handling.

The switchover system consists of two signaling controllers connected through IP, as shown in Figure 3-1. One SC functions as the active host, while the other SC functions as the standby host. The switchover system provides a seamless transition to the standby host in case of system failures.

The active host maintains communications between the active and standby hosts. The standby host constantly checks the active host for new and changed configurations and updates itself on a regular basis. When the standby host becomes the active host, its configuration mirrors that of the former active host without losing the link with the NAS, thus preserving calls.

Figure 3-1 Switchover Processes on the Signaling Controller Hosts



System Messages

The Cisco Signaling Controller software generates system messages that provide you with call processing, management, configuration and alarm status.

Status messages include these types:

- Man-Machine Language (MML) responses

  After you enter an MML command, one of the following messages is generated: MML status, MML error code, auto-generated or autonomous, and alarm.

- Portable Execution Environment (PXE) log messages

  The Portable Execution Environment (PXE) logging system sends messages to log files determined during the client initialization period.

  The PXE log server software takes messages initiated by various applications (other software processes) within the Cisco Signaling Controller software, formats the messages, and sends them to the appropriate files. The PXE log server also adds a time stamp, an application identifier (also known as a service ID or service name), a process identifier (that is, the UNIX process), and a log level.

- Cisco Signaling Controller console messages generated by the UNIX operating system

For detailed information about system messages, see these Cisco SS7 Interconnect for Voice Gateways Solution documents:

- *Cisco Media Gateway Controller Software Release 7 Operations, Maintenance, and Troubleshooting Guide*
- *Cisco Media Gateway Controller Software Release 7 Reference Guide*

Call Detail Recording (CDR)

CDRs are comprised of call data elements (CDEs). The CDE is the data element (field) that includes a basic information field within a billing record. Examples of CDEs are the calling number, called number, and so on. The call data block (CDB) consists of several CDEs, related to a certain point in call (PIC).

New data elements are added to the CDBs as results from Cisco system enhancement or from special customer-oriented CDB design. For example, a new TLV (Time, Length, and Value) element is added to comply to NTT (Nippon Telephone and Telegraph) CDR requirement.

For detailed information about CDEs and CDBs and an overview of the Cisco Signaling Controller billing system, see these Cisco SS7 Interconnect for Voice Gateways Solution documents:

- *Cisco Media Gateway Controller Software Release 7 Operations, Maintenance, and Troubleshooting Guide*
- *Cisco Media Gateway Controller Software Release 7 Installation and Configuration Guide*

Disk Mirroring

Disk mirroring is a feature that duplicates the information contained in a file system by using two disk partitions located on separate physical disks. In the event of a physical disk failure, the file system continues to operate using the unaffected disk.

Disk mirroring is used on fault-tolerant configurations with the Sun Netra t 140x server platform. This feature increases the availability of the Cisco SC2200 by keeping the system operating when a physical disk fails—a mirrored disk can be removed and replaced while the system remains active. With redundant SC hosts using disk mirroring, a single disk failure does not cause switchover, as described in the "Understanding System Redundancy" section.

The Volume Manager software running on your Cisco SC2200 provides this feature in a transparent manner so that the application software does not know that there are multiple disk partitions making up the file system.

For detailed information about how to install disk mirroring through Volume Manager, see the *Cisco Media Gateway Controller Software Release 7 Installation and Configuration Guide*.

Note Disk mirroring is optional on the Sun Netra t 112x and Sun Ultra E450 server platforms.

Manual Control Options

The Cisco Signaling Controller includes two tools that you can use to provision the software: the Cisco MGC Manager (CMM) graphical user interface (GUI) application and the Man-Machine Language (MML) Command Line Interface (CLI) application.

CMM makes provisioning easier for less-experienced administrators by listing all the components that need to be configured and by providing windows that display all configuration parameters for each component. Instructions for provisioning with CMM can be found in the *Cisco Media Gateway Controller Software Release 7 TCM Provisioning Guide*.

Although MML provisioning requires more keystrokes, quick provisioning updates can sometimes be made faster with MML commands, because you do not have to go through the process of launching CMM. MML commands entered into a text file can be batched from the UNIX command line to speed up provisioning, and you can copy and modify MML scripts to configure additional MGC switches. For information on provisioning with MML, refer to the *Cisco Media Gateway Controller Software Release 7 MML Provisioning Guide*.

You can use both CMM and MML to provision the Cisco Signaling Controller. However, you can use only one of these tools at a time for actual configuring. Table 3-1 lists some of the features of CMM and MML and provides guidelines for selecting between the two tools.

Table 3-1 CMM and MML Features

Specifications/Features	CMM	MML
System Basics	X-windows GUI front end, SNMP back end	CLI that interacts directly with the Cisco Signaling Controller.
System Hardware/Software Requirements	• SC host server running Solaris 2.6 • Running the TCM on the same server as the Cisco Signaling Controller can adversely impact performance. Cisco recommends using a separate server.	Runs on the SC host server.
Batch File Support	No	Yes
Level of Network/Telephony Experience Required	Little experience required; very easy to use.	Requires a high level of experience with MML and the Cisco Signaling Controller software.
Best Used For	• Setting up a single configuration or few configurations on individual SC host servers. • Modifying an existing configuration.	• Creating batch files to configure many SC host servers or retrieve measurements. • Modifying configurations (experienced users). • Scaling large configurations.

CHAPTER 4

Implementation Overview

This chapter describes how to implement the Cisco SS7 Interconnect for Voice Gateways Solution by installing and configuring the components. The following sections describe the tasks:

Implementation Task List

To implement your Cisco SS7 Interconnect for Voice Gateways Solution, you must:

Step 1 Design your network by identifying the physical configuration and components of your network. This network design should be based on assumptions that meet your network requirements. Plan your design to include the following:

- Signaling routes to external switches
- Signaling links to signaling points
- Network access server control links
- Trunks, trunk groups, and QoS packet network routes

See the *Cisco Media Gateway Controller Software Release 7 Provisioning Guide* for details.

Step 2 Create a dial plan. See the *Cisco Media Gateway Controller Software Release 7 Provisioning Guide* for details.

Step 3 Connect the signaling controller hardware. See the "Hardware Installation" section for details.

Step 4 Connect the Cisco SLT and LAN switch to the signaling controller. See the "Hardware Installation" section for details.

Step 5 Install the operating system software and signaling controller software on the signaling controller host. See the "Signaling Controller Software Installation" section for details.

Step 6 Configure the software on the signaling controller. See the "Configuring the Signaling Controller" section for details.

a. Assign an IP address to the signaling controller and then create and deploy the configuration file on the signaling controller.

b. Configure the TCM server and assign an IP address to the server.

Step 7 Configure the software on the Cisco SLT. See the "Configuring the Cisco SLT" section for details.

Step 8 Configure the software on the LAN switch. If you are using a Cisco Catalyst switch, see the "Configuring the LAN Switch (Optional)" section for details.

Step 9 Install the access gateway. See the "Gateway Installation and Configuration" section for details.

a. Connect the access gateway to the LAN switch.

b. Connect the access gateway to the Public Switched Telephone Network (PSTN).

c. Configure and assign IP addresses to the access gateways. See the section "Gateway Installation and Configuration" for details.

Step 10 Configure the network management system, if installed for your Cisco SS7 Interconnect for Voice Gateways Solution, for its connectivity with the Cisco SC2200.

Step 11 Make sure that all the devices can talk to each other by pinging one device from another. For example, you should be able to ping the media router and the DNS server (node in the Internet cloud) from each device. You should also be able to access (using Telnet, ReflectionX, or other such software) each device from the other devices.

Hardware Installation

This section provides an overview of the recommended hardware connection sequence. For details, refer to the appropriate hardware installation guide. Make sure that you have the hardware installation guides handy for all the devices you are connecting in your system.

Signaling Controller Installation

Installing the signaling controller hardware involves wiring the signaling controller in this sequence:

	Task	Reference
Step 1	If using dedicated DC power, connect the power supply to the signaling controller.	*Cisco Media Gateway Controller Hardware Installation Guide*
Step 2	Connect the LAN switch to your LAN. **Note** The LAN switch is not provided with the signaling controller.	
Step 3	Connect a console terminal to the signaling controller using an EIA/TIA-232 cable.	
Step 4	Connect the signaling controller to the IP network to which the access gateways will be connected. **Note** The IP signaling network is a separate network from the H.323 voice network.	

Cisco SLT Installation

Installing the SLT hardware involves connecting the Cisco SLTs in this sequence:

	Task	Reference
Step 1	Connect serial ports through the T1/E1, V.35, EIA/TIA-449, or EIA/TIA-530 interfaces to the STPs.	• *Cisco Media Gateway Controller Hardware Installation Guide* • Cisco IOS Release 12.1(2)T documentation, *Cisco Signaling Link Terminal*
Step 2	Connect Ethernet ports through the Ethernet 10BASE-T to the signaling controller or the LAN switch.	

Network Access Installation

Installing the network access hardware involves the following:

	Task	Reference
Step 1	If you have one IP network, connect the access gateways to the LAN switch. If you have two IP networks, use the access gateway Ethernet port to connect each access gateway to the POP management network, and use the access gateway Fast Ethernet port to connect each access gateway to the IP data network.	*Cisco Media Gateway Controller Hardware Installation Guide*
Step 2	Connect the bearer channels to the access gateway using RJ-48 connections for the T1/E1/T3 interfaces.	

Signaling Controller Software Installation

This section provides an overview of the recommended hardware connection sequence. For details, refer to the appropriate hardware installation guide. Make sure that you have the hardware installation guides handy for all the devices you are connecting in your system.

	Task	Reference
Step 1	Install the operating system on the signaling controller: **a.** Verify SC host firmware. **b.** Verify that the Sun Solaris operating system is installed appropriately. **c.** Install the Volume Manager. **d.** Create the Log and Spool volumes.	*Cisco Media Gateway Controller Software Release 7 Installation and Configuration Guide*
Step 2	Install the Cisco SC host software: **a.** Install the software for a single-host or dual-host configuration. **b.** Configure the execution environment. **c.** Terminate the signaling links. **d.** Configure the SNMP support resources.	
Step 3	Install Cisco IOS on the Cisco SLT. To determine the correct software release version, refer to *Release Notes for Cisco Media Gateway Controller Software Release 7*.	• *Cisco Media Gateway Controller Software Release 7 Installation and Configuration Guide* • *Release Notes for Cisco Media Gateway Controller Software Release 7*

Signaling Controller Software Configuration

Configuring the signaling controller software consists of three tasks:

- Configuring the Signaling Controller
- Configuring the Cisco SLT
- Configuring the LAN Switch (Optional)

Configuring the Signaling Controller

Caution Always use the Cisco signaling controller CMM tool or MML commands to create, modify, manage, and deploy your configuration files on the signaling controller. Cisco does not recommend modifying the configuration files directly on the signaling controller.

Configuring the signaling controller includes these steps:

	Task	Reference
Step 1	Prepare the following: • Bearer routes to other switches • Signaling point links • Network access server control links • Trunks, trunk groups, and routes • Dial plans	*Cisco Media Gateway Controller Software Release 7 Installation and Configuration*
Step 2	Configure the SS7 signaling routes to external switches by completing the following tasks: • Add the OPC in your network. • Add the DPC to identify the destination switch. • Add the APCs to identify the STPs with which the signaling controller communicates signaling information. • Add linksets to connect the Cisco SLTs to the STPs. • Add the SS7 subsystem to identify the mated STPs. • Add the SS7 routes for each signaling path from the signaling controller to the destination switch. • Add the SS7 signaling service from the signaling controller to the destination switch.	*Cisco SS7 Interconnect for Access Servers and Voice Gateways Solutions Provisioning Guide*
Step 3	Provision the signaling links by completing the following tasks: • Add the Ethernet adapters (cards) in the SC host that carry signaling to and from the Cisco SLTs. • Add Ethernet interfaces for the cards in the host. • Add C7 IP links for each SS7 link from the signaling controller to the SS7 network (through the Cisco SLT).	

	Task	Reference
Step 4	Configure the access gateway control links by completing the following tasks: • Add external nodes for the access gateways in your network. • Add NAS signaling services for each access gateway. • Add IP links for each access gateway to each Ethernet card in the SC host.	*Cisco SS7 Interconnect for Access Servers and Voice Gateways Solutions Provisioning Guide*
Step 5	Configure trunks, trunk groups, and routes.	
Step 6	Provision black and white trunk screening.	
Step 7	Build and deploy the configuration.	

Configuring the Cisco SLT

Configuring the Cisco SLTs includes these steps:

	Task	Reference
Step 1	Identify the serial WAN interface card on your Cisco SLT and connect cable to card as described in Steps 1 and 2 of the "Cisco SLT Installation" section on page 4-3.	*Cisco Media Gateway Controller Software Release 7 Installation and Configuration Guide*
Step 2	Install the Cisco SLT image software.	
Step 3	Configure the basic parameters and SS7 links for the Cisco SLT.	
Step 4	Configure Session Manager and RUDP.	
Step 5	Save the new configuration as the startup configuration, and then reload the Cisco SLT.	

For additional details, refer to the following documents:

- *Quick Start Guide Cisco 2600 Series Cabling and Setup*
- *Cisco 2600 Series Hardware Installation Guide*
- *Cisco Network Module Hardware Installation Guide*
- *Cisco 2600 WAN Interface Cards Hardware Installation Guide*
- *Software Configuration Guide for Cisco 2600 and Cisco 3600 Series Routers*
- *New and Changed Show Commands for Cisco 2600 Series Routers*
- *Cisco 2600 Series Configuration Notes*

Tip The Cisco publications are available online on the Cisco website or on the Cisco Documentation CD-ROM that arrived with your system.

Configuring the LAN Switch (Optional)

This section describes the task of configuring LAN switches (Cisco Catalyst Switch family) for your solution. The LAN switch connects the SC hosts to the access gateways or the Cisco SLTs. The LAN switch is used in the SC node to extend VLANs across platforms through backbone Fast Ethernet, Gigabit, or ATM connections, when necessary. The LAN switch is not provided with the SC host. Configuring the LAN switch includes these steps:

	Task	Reference
Step 1	Make sure that you have virtual LAN assignments and IP address assignments for solution devices.	*Cisco Media Gateway Controller Software Release 7 Installation and Configuration Guide*
Step 2	Configure basic system information.	
Step 3	Configure the logical interface.	
Step 4	Configure SNMP information.	
Step 5	Configure the virtual LANs (VLANs).	
Step 6	Configure module and port parameters.	
Step 7	Configure spanning-tree parameters.	
Step 8	Configure the standby ports.	
Step 9	Configure the ISL connections between switches.	
Step 10	Configure the Switch Port Analyzer.	
Step 11	Configure the Route Switch Module.	

Gateway Installation and Configuration

To install the voice gateway, perform the following tasks:

	Task	Reference
Step 1	Rack-mount the access gateway chassis.	*Cisco SS7 Interconnect for Access Servers and Voice Gateways Solutions Media Gateway Guide*
Step 2	Connect the access gateway to the network as described in Steps 1 and 2 of the "Network Access Installation" section on page 4-4.	
Step 3	Connect a console terminal and auxiliary ports.	
Step 4	Supply power to the access gateway.	

For each access gateway installed in your Cisco SS7 Interconnect for Voice Gateways Solution, configure the access gateway by performing the following tasks:

	Task	Reference
Step 1	Configure the switch type to NI2, using the **isdn switch-type primary-ni** command. (This command enables the connection between the access gateway and the virtual switch controller.)	*Cisco SS7 Interconnect for Access Servers and Voice Gateways Solutions Media Gateway Guide*
Step 2	Configure the access server for channelized T1/E1/T3 lines.	

To install the optional access gateway software features supported on your Cisco SS7 Interconnect for Voice Gateways Solution, perform the following tasks:

	Task	Reference
Step 1	Configure Continuity Testing (COT)	Cisco IOS Release 12.0(3)T documentation • *Continuity Testing (COT)*
Step 2	Configure the Redundant Link Manager (RLM)	*Cisco SS7 Interconnect for Access Servers and Voice Gateways Solutions Media Gateway Guide* Cisco IOS Release 12.0(7)XR documentation • *Cisco H.323 VoIP with SS7 for the Cisco AS5300*

To install and configure Voice-over-IP on your Cisco SS7 Interconnect for Voice Gateways Solution, see the following reference documentation:

Reference
Voice-over-IP for the Cisco AS5300 Universal Access Server Software Configuration Guide

Gatekeeper Installation and Configuration (Optional)

Your Cisco SS7 Interconnect for Voice Gateways Solution may include a gatekeeper. To install and configure Voice over IP on the Cisco 3640 gatekeepers, see the following reference documentation:

Reference
Cisco IOS Release 12.1 *Voice, Video, and Home Applications Configuration Guide*
Cisco IOS Release 12.1 *Voice, Video, and Home Applications Command Reference*

Operation and Maintenance

Under normal conditions, the primary (active) signaling controller application (MTP3 and the Call Processing Engine) processes calls. In addition to normal call processing, in a fault-tolerant configuration the primary signaling controller updates the standby signaling controller with call state information when a call enters the establish phase. This ensures that the call state is maintained in case of failure.

The following are normal operating procedures for the signaling controller. For detailed instructions on these operation procedures and maintenance tasks, see the *Cisco Media Gateway Controller Operations, Maintenance, and Troubleshooting Guide*.

- Managing signaling channels and lines
- Managing traffic channels
- Managing switchover

The following are operating procedures under various equipment failure scenarios:

- Signaling link termination failure
- Call processor failure
- Operating system failure
- LAN switch failure

The following are maintenance tasks necessary for each component in your Cisco SC2200:

- Checking equipment status
- Preventive maintenance
- Removing the component from your system
- Replacing the component

Configuring Other Components

Refer to the documentation that shipped with a particular component for configuration information.

If You Need More Information

The Cisco IOS software running on your router contains extensive features and functionality. The effective use of many of these features is easier if you have more information. For additional information on configuring and maintaining a signaling controller, see the "Obtaining Documentation" section on page xi and the "Obtaining Technical Assistance" section on page xii.

SS7 Technology

Overview

SS7 is a set of standards for the Common Channel Signaling (CCS) system. Historically, SS7 defines the architecture, network elements, interfaces, protocols, and management procedures for a Public Switched Telephone Network (PSTN) that transports control information between network switches and between switches and databases. SS7 is used between the PSTN switches; replacing per-trunk, in-band signaling.

Typically, SS7 is implemented on a separate data network within the PSTN and provides call setup and teardown, network management, fault resolution, and traffic management services. The SS7 network is used solely for network control, and the only data sent over it is signaling messages.

Note The term SS7 can be used to refer to the SS7 protocol, the signaling network, or the signaling network architecture.

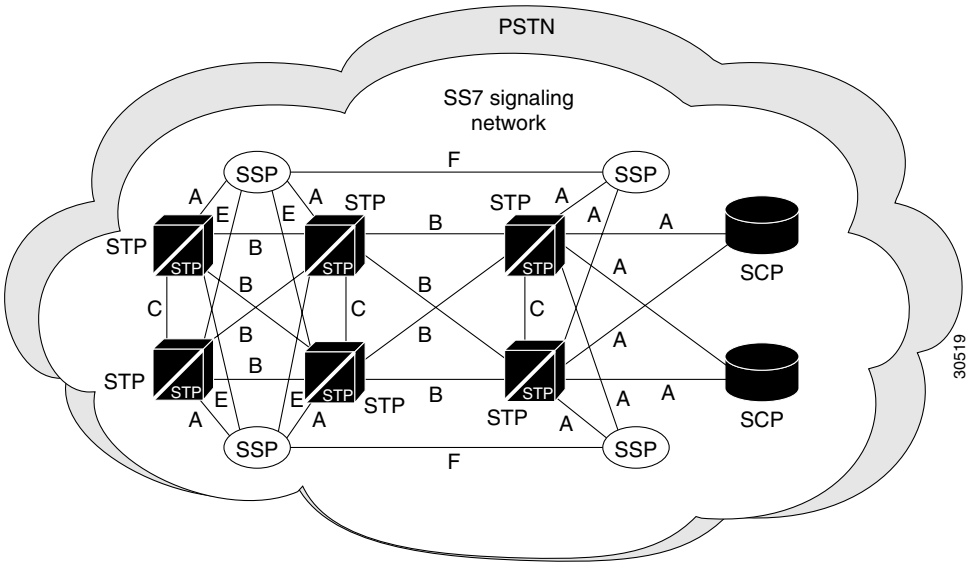
The SS7 protocols that convey signaling information between switching systems (called signaling points) in the PSTN are carried on a special overlay network used exclusively for signaling. The signaling points use routing information in the SS7 signals to transfer calls to their final destinations.

The SS7 network features include:

- Control over the establishment of calls across the PSTN.
- Routing, billing, information exchange functions, specialized call treatments, and enhanced routing.
- Common channel signaling in which signaling information for different connections travels on separate dedicated signaling channels.
- Voice and data connections that travel on bearer channels.

Figure A-1 is a graphic representation of SS7 links and how they are used in an SS7 signaling network.

Figure A-1 SS7 Signaling Network



The SS7 architecture consists of the following signaling points (as shown in Figure A-1):

- Service Switching Points (SSPs) are telephone switches equipped with SS7 software and signaling links. Each SSP is connected to both STPs in a mated pair.
- Signal Transfer Points (STPs) receive and route incoming signaling messages toward their destinations. STPs are deployed in mated pairs and share the traffic between them.
- Service Control Points (SCPs) are databases that provide the necessary information for special call processing and routing, including 800 and 900 call services, credit card calls, local number portability, cellular roaming services, and advanced call center applications.

As you can see in Figure A-1, the SCPs and STPs and their links are deployed as mated pairs because of the critical nature of the signaling network.

Point Codes

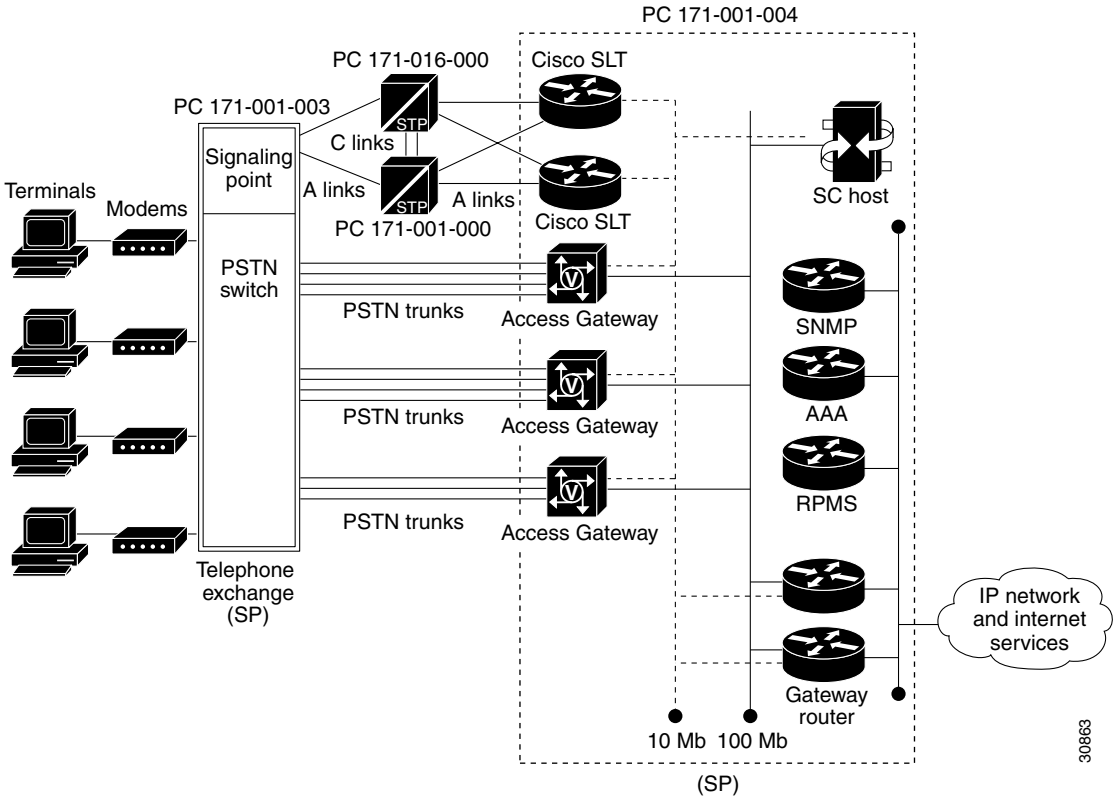
Each signaling point (also called an SS7 node or SP) in the SS7 network is identified with a unique address called a point code (PC). ANSI point codes are 24-bit and ITU point codes are 14-bit. PCs are carried in signaling messages exchanged between signaling points to identify the source and destination of each message. PCs are managed by the government agency that supervises, licenses, and controls electronic and electromagnetic transmission standards in your country. Note that there could be two separate agencies managing policy and providing licenses in your country.

Note When using STPs, multiple signaling links between the same nodes (point-to-point) share traffic and are referred to as linksets.

The ANSI point code is a hierarchical address consisting of:

- Network identification—Identifies a signaling network.
- Network cluster—Identifies a cluster of nodes belonging to a signaling network. For example, you can address a group of nodes by using the same mated pair of STPs as a network cluster.
- Network cluster member—Identifies a single signaling point within a cluster.

Figure A-2 Point Codes in the SS7 Network



In Figure A-2, C-links (cross links) connect STPs together to form mated pairs (PC 171-016-000 and PC 171-001-000). A-links (access links) connect STPs with the telephone exchange signaling point (PC 171-001-003) and with the redundant pair of Cisco SLTs of the
Cisco SS7 Interconnect for Voice Gateways Solution signaling point.

Note These point codes are in ANSI SS7 point code format. Variations of SS7 might use different point code formats. The network-cluster-member format is only valid with ANSI SS7 point code formats.

The PC 171-016-000 used for one of the mated STPs consists of the following elements:

- 171 is the network identification.
- 016 is the network cluster representing only the top STP in Figure A-2.
- 000 is the network cluster member, which is connected to the network cluster.

Reference Documentation

See the following publications and web site for a comprehensive overview of SS7:

- Black, U. *ISDN and SS7 Architecture for Digital Signaling Networks.* Upper Saddle River, New Jersey: Prentice Hall PTR; 1997.
- Bellamy, J. *Digital Telephony*, Second Edition. New York, New York; John Wiley and Sons, Inc.; 1991.
- http://www.iec.org/. Click **Training**, **Web ProForum Tutorials**, **Communications Networks**, and then scroll down the list and click **Signaling System #7 (SS7**).
- Russel, T. *Signaling System #7*, Third Edition. McGraw-Hill; 2000.

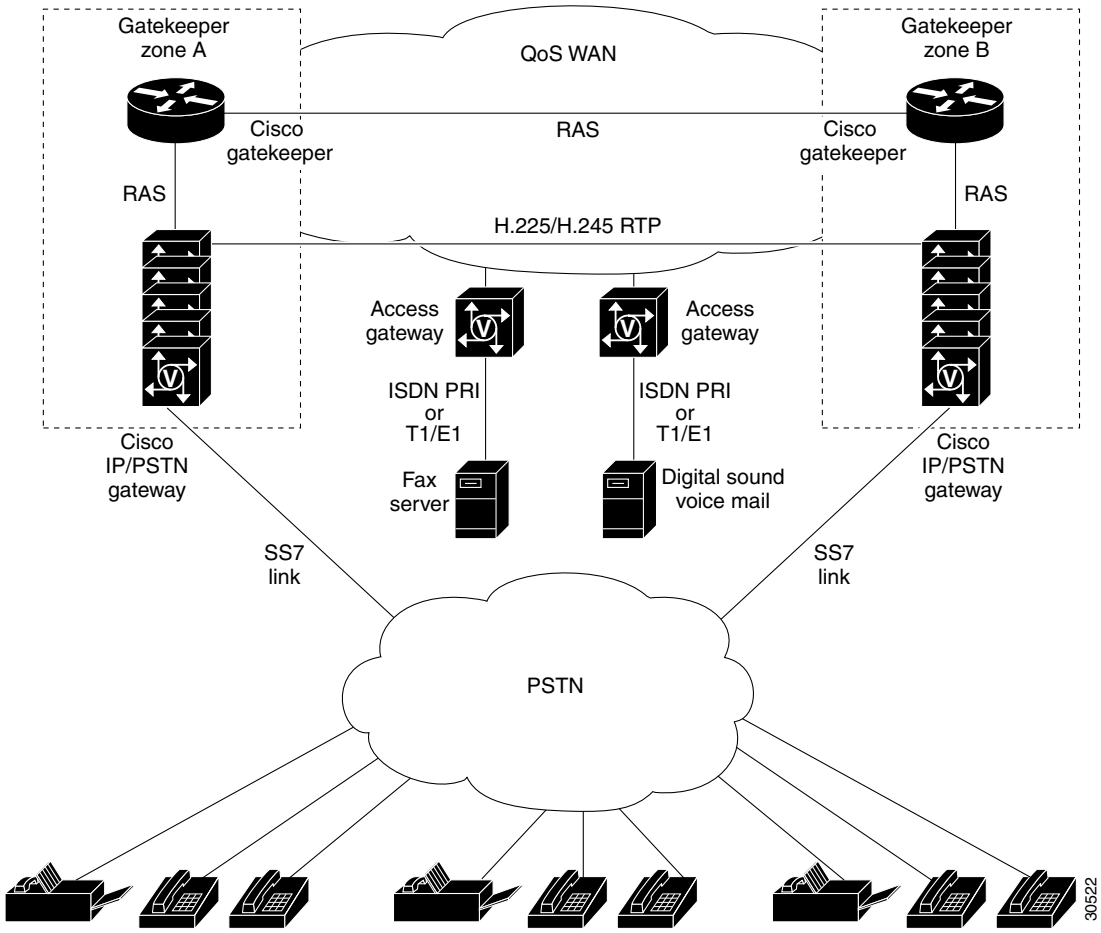
Voice-over-IP

Overview

The Cisco SS7 Interconnect for Voice Gateways Solution builds on existing Cisco H.323 Voice over IP (VoIP) architecture that consists of a Cisco AS5*x*00 access gateway and Cisco 2600 series or Cisco 3600 series routers operating as gatekeepers within an H.323 infrastructure. This architecture provides the quality of service (QoS), stability, and functionality necessary for carrier class, real-time IP communications services.

Figure B-1 illustrates the gateway and gatekeeper internetworking functionality in detail.

Figure B-1 VoIP PSTN Signaling Architecture



How VoIP Processes a Telephone Call

It helps to understand what happens at an application level when you place a call using VoIP. The general flow of a two-stage voice call using VoIP is as follows:

Step 1 The user picks up the handset; this signals an off-hook condition that is generated by the PBX or end-office SSP in the PSTN.

Step 2 The SSP provides digit analysis and route determination, then generates dial tone and sends an IAM to the signaling application part of VoIP in the gateway.

Step 3 The VoIP issues an alerting/ACM that indicates to the SSP to start the dial tone or busy tone (based on the state of the receiving end).

Step 4 Upon dial tone, the user dials the telephone number; those numbers are accumulated and stored by the session application.

Step 5 After enough digits are accumulated to match a configured destination pattern, the telephone number is mapped to an IP host through the dial plan mapper. The IP host has a direct connection to either the destination telephone number or a PBX that is responsible for completing the call to the configured destination pattern.

Step 6 The session application then runs the H.323 session protocol to establish a transmission and a reception channel for each direction over the IP network. If the call is being handled by a PBX, the PBX forwards the call to the destination telephone. If Resource Reservation Protocol (RSVP) has been configured, the RSVP reservations are put into effect to achieve the desired quality of service (QoS) over the IP network.

Step 7 The codecs are enabled for both ends of the connection and the conversation proceeds using RTP/UDP/IP as the protocol stack.

Step 8 Any call-progress indications (or other signals that can be carried in-band) are cut through the voice path as soon as an end-to-end audio channel is established. Signaling that can be detected by the voice ports (for example, in-band dual tone multifrequency [DTMF] digits after the call setup is complete) is also trapped by the session application at either end of the connection and carried over the IP network encapsulated in RTP Control Protocol (RTCP), using the RTCP APP extension mechanism.

Step 9 When either end of the call hangs up, the RSVP reservations are torn down (if RSVP is used) and the session ends. Each end becomes idle, waiting for the next off-hook condition to trigger another call setup.

Key Elements

The key elements of the H.323 VoIP architecture are:

- Gateways
- Gatekeepers
- Gatekeeper Zones
- H.323 Terminals

Gateways

In the Cisco H.323 VoIP with SS7 Solution, the Cisco AS5300 operates as the VoIP gateway and dial-up remote access server. When equipped with voice feature cards (VFCs) and voice-enabled Cisco IOS software the Cisco AS5300 supports carrier-class VoIP and fax over IP services.

Gateways allow H.323 terminals and routers to communicate with terminals running other protocols. They provide protocol conversion between terminals and routers running different types of protocols. A gateway is the point at which a circuit-switched call is encoded and repackaged into IP packets.

An H.323 gateway is an endpoint on the LAN that provides real-time, two-way communications between H.323 terminals on the LAN and other H.323 terminals in the WAN, or to another H.323 gateway.

A VoIP gateway has two primary applications. It can terminate a call from the PSTN and provide user admission control using integrated voice response (IVR) and provide accounting records for the call. The gateway also can direct the call to the destination or can terminate the call from another gateway and send the call to the PSTN. The gateway (in this document) refers to the voice-capable platform with voice cards and the VoIP image.

Figure B-2 and Figure B-3 illustrate these two applications. The VoIP gateway used in this solution is the Cisco AS5300.

Figure B-2 VoIP Used as a PSTN Gateway for Internet Telephone Traffic

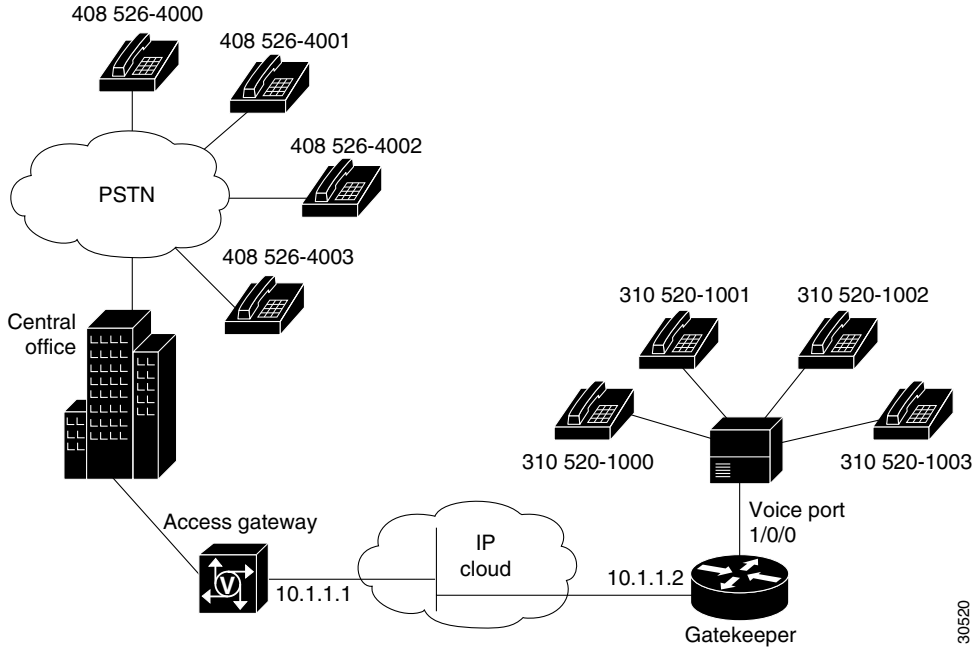
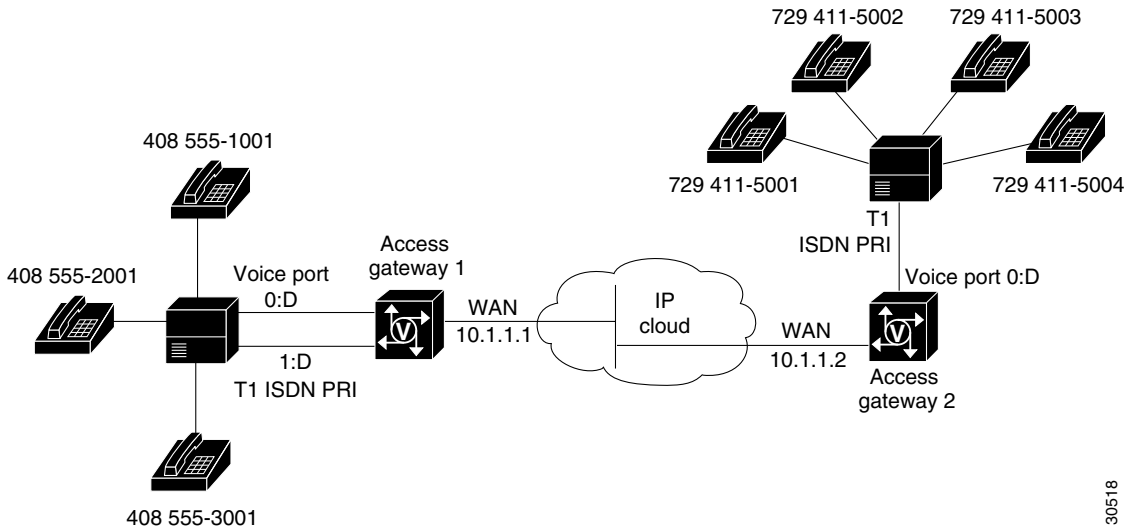


Figure B-3 VoIP Gateway Used as a Central Site Telephony Termination Facility



Gatekeepers

Gatekeepers are optional nodes that manage other nodes in an H.323 network. Other nodes communicate with the gatekeeper using the Registration, Admission, and Status (RAS) protocol.

These nodes register with a gatekeeper on startup. When they wish to communicate with another endpoint, they request admission to the call, using a symbolic alias for the endpoint name, such as an E.164 address or an e-mail ID. If the gatekeeper decides that the call can proceed, it returns a destination

IP address to the originating endpoint. This IP address can be the actual address of the target endpoint, or it can be an intermediate address. Finally, a gatekeeper and its registered endpoints exchange status information.

Gatekeeper Zones

H.323 endpoints are grouped together in zones. Each zone has one gatekeeper that manages all of the endpoints in the zone. A zone is an administrative convenience similar to a DNS domain.

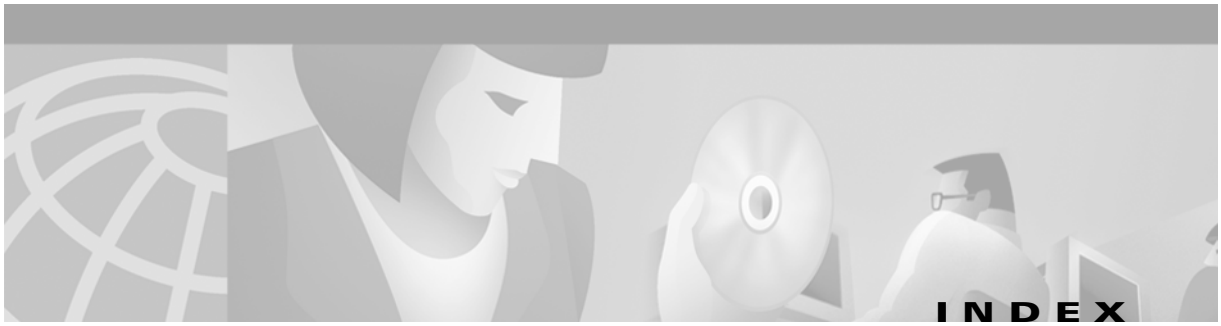
H.323 Terminals

An H.323 terminal is an endpoint in the LAN that provides for real-time, two-way communications with another H.323 terminal or gateway. This communication consists of control, indications, audio, moving color video pictures, or data between the two terminals. A terminal may provide audio only; audio and data; audio and video; or audio, data, and video.

Reference Documentation

See the following publications for detailed information:

- *Service Provider Features for Voice over IP*
- *Voice over IP for the Cisco AS5300 Universal Access Server*
- *Voice over IP for the Cisco AS5800 Universal Access Server*



A

B

C

D

E

F

G

H

I

L

M

N

O

P

R

S

T

U

V