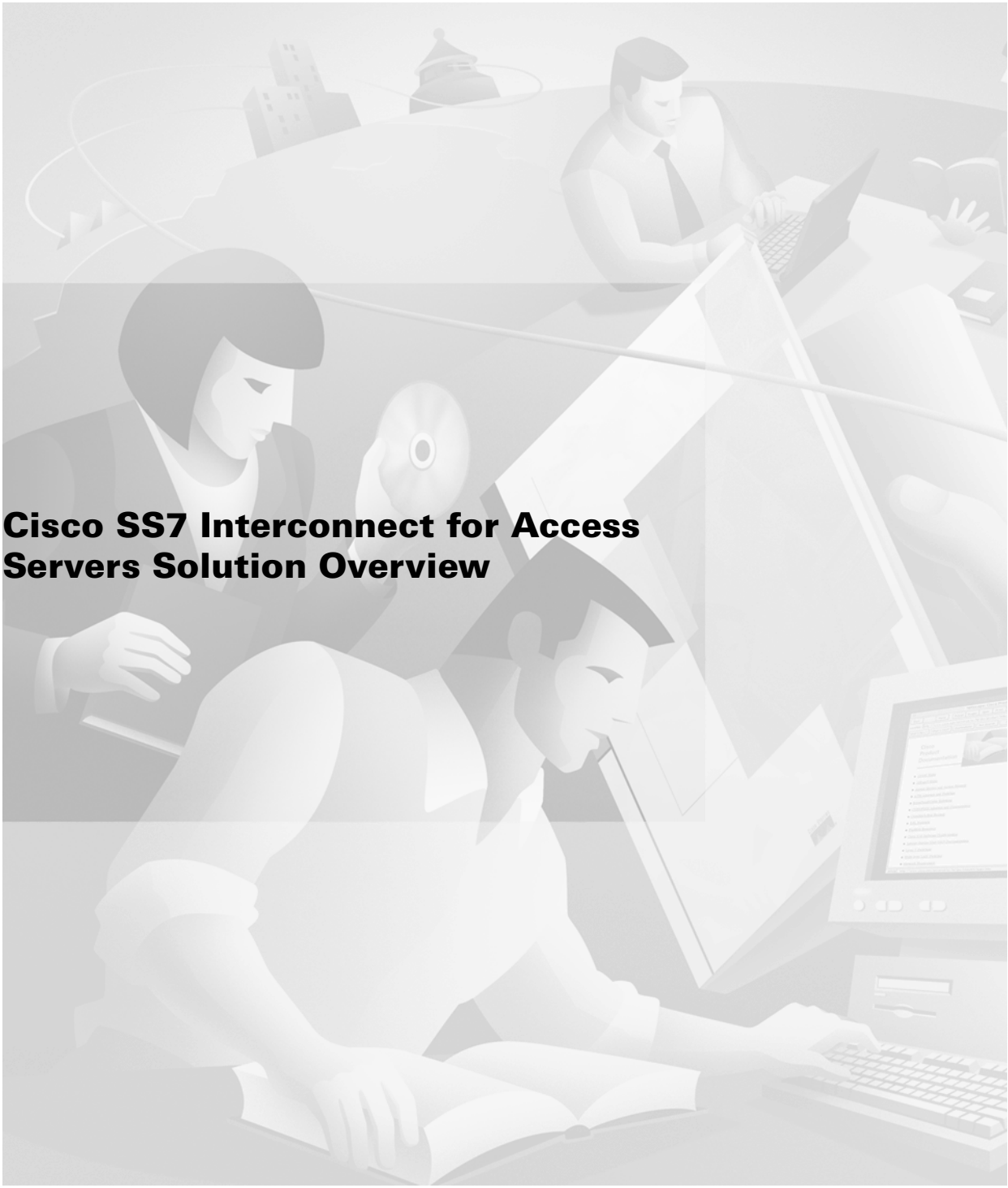


Cisco SS7 Interconnect for Access Servers Solution Overview

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

Customer Order Number:
Text Part Number: 78-10288-02

Cisco SS7 Interconnect for Access Servers Solution Overview

Preface

This section describes the objectives, audience, organization, and conventions of the Cisco SS7 Interconnect for Access Servers Solution. The guide points to related publications and describes online sources of technical information.

Document Objectives

This guide is designed to provide you with an overview of the Cisco SS7 Interconnect for Access Servers 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 guide is intended as part of a suite of documents for the following users. (See the Cisco SS7 Interconnect for Access Servers Documentation Map, page vii.)

- Component installers—Who have experience installing telecommunications equipment and cabling, as well as experience installing data communications equipment and cabling.
- Network operators/administrators—Who have experience in telecommunications networks, protocols, and equipment, as well as a familiarity with data communications networks, protocols, and equipment.
- Network designers—Who have experience with telecommunications networks, protocols, and equipment, as well as experience with data communications networks, protocols, and equipment.

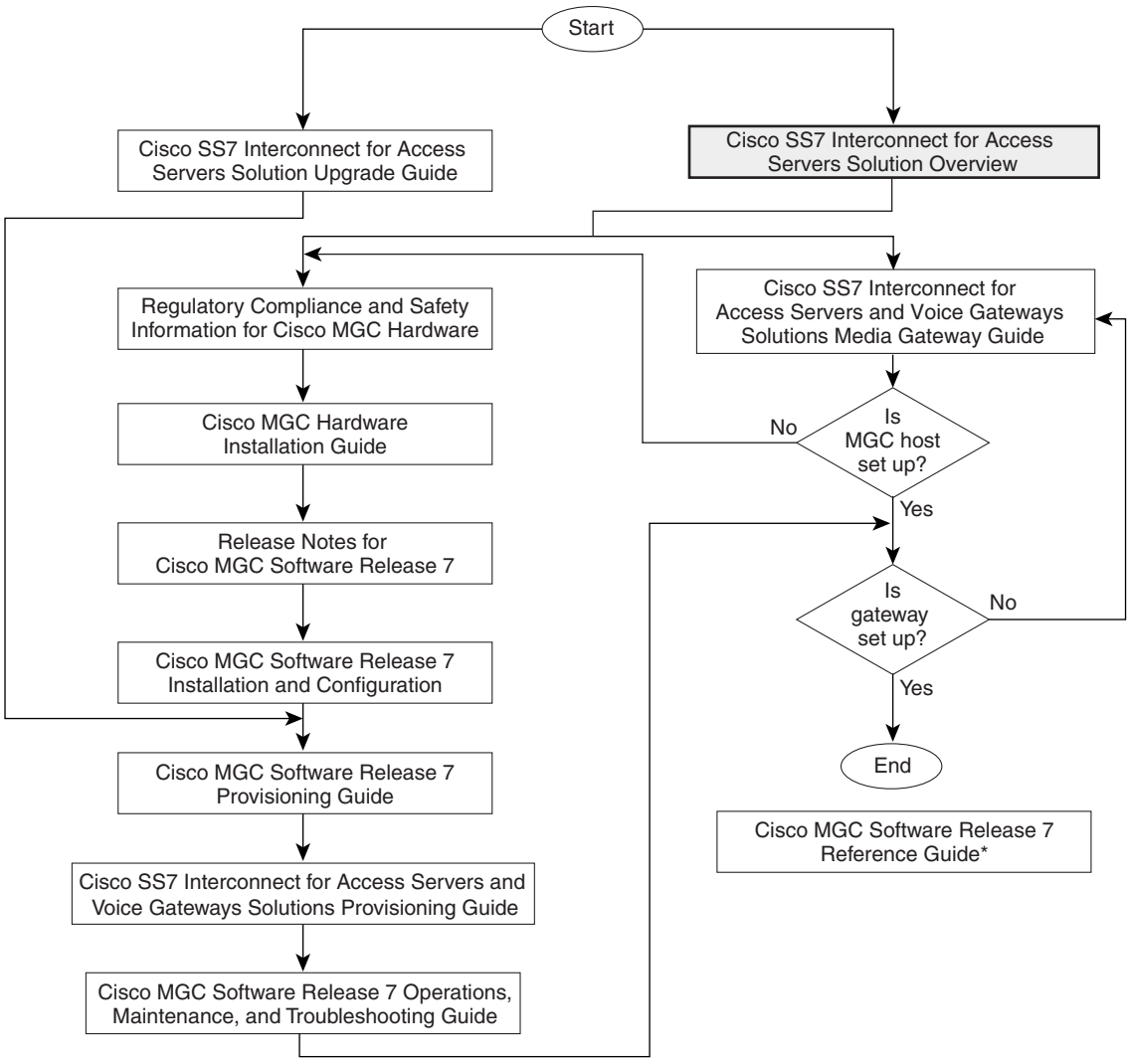
Document Organization

The major sections of this document are as follows:

Chapters	Title	Description
Chapter 1	Cisco SS7 Interconnect for Access Servers Solution Introduction	Provides an introduction to the Cisco SS7 Interconnect for Access Servers Solution, describes architecture, benefits, features, and applications.
Chapter 2	Cisco SS7 Interconnect for Access Servers Configuration Options and Components	Provides information about configuration options and brief description of components.
Chapter 3	Cisco SS7 Interconnect for Access Servers Solution Operations	Describes unattended operations and manual control options.
Chapter 4	Cisco SS7 Interconnect for Access Servers Solution Implementation	Provides sequence of implementation steps for the Cisco SS7 Interconnect for Access Servers system, the hardware connections, and software installation. Also, provides high-level component configuration steps with pointers to detailed documents.
Appendix A	SS7 Technology Overview	Provides a brief overview of SS7 technology used in this guide.

Cisco SS7 Interconnect for Access Servers Documentation Map

Refer to the following documentation map to navigate through the Cisco SS7 Interconnect for Access Servers 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.

Cisco SS7 Interconnect for Access Servers Documentation Suite

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

- *Cisco SS7 Interconnect for Access Servers Solution Upgrade Guide*
- *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 Media Gateway Controller Software Release 7*

Refer to the following document for detailed Cisco IOS documentation about the Cisco SS7 Interconnect for Access Servers Solution:

- *Cisco IOS Release Notes for the Cisco SS7 Interconnect for Access Servers*

Document Conventions

Table 1 SS7 Interconnect for Access Servers 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.
[ ]	Default responses to system prompts appear in square brackets.

Table 1 SS7 Interconnect for Access Servers Overview Conventions (continued)

Convention	Description
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.

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

Cisco SS7 Interconnect for Access Servers Solution Introduction

Overview

The Cisco SS7 Interconnect for Access Servers Solution is a distributed system that interconnects Cisco network access servers (NASs) to a circuit-switched TDM network using the Signaling System 7 (SS7) protocol. The interconnections are achieved using a protocol conversion platform called the Cisco SC2200 combined with the Cisco Signaling Link Terminal (SLT). The Cisco SC2200 consists of a hardware and software package that provides the signaling controller function in the Cisco SS7 Interconnect for Access Servers Solution. It provides high availability, high performance, and key scaling.

When large points of presence (POPs) receive calls from the Public Switched Telephone Network (PSTN), the traffic runs over legacy architectures that use in-band signaling (such as Integrated Services Digital Network Primary Rate Interfaces (ISDN PRIs), in-band channel-associated signaling (CAS), or single analog lines) rather than out-of-band signaling like SS7. With both signaling and bearer traffic running over the lines, these legacy switches become congested with modem traffic and limited circuits. Cisco offers the Cisco SS7 Interconnect for Access Servers Solution that offloads the signaling to an out-of-band network so that available bandwidth increases.

The Cisco SS7 Interconnect for Access Servers Solution is a distributed system that adds SS7 signaling interfaces to large ISP POPs. SS7 interfaces are connected to the PSTN by using the same signaling technology as a PSTN switch. The Cisco SS7 Interconnect for Access Servers Solution consists of the Cisco SC2200, the Cisco SLT, and the NASs. The Cisco SS7 Interconnect for Access Servers Solution turns a POP into an end-office switching system in the PSTN, allowing direct peer-to-peer signaling connectivity. The POP, as a switch, connects directly to the rest of the network as a peer. After connections to the Internet are aggregated at a POP, streams of user packets are statistically multiplexed for efficient transport over the backbone network.

Figure 1-1 illustrates the PSTN-to-POP network without a Cisco SS7 Interconnect for Access Servers Solution. Because of Internet and additional data calls with hold times that average 30 minutes, the PSTN network experiences more busy signals and overloads network resources.

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

Figure 1-1 Without the Cisco SS7 Interconnect for Access Servers Solution

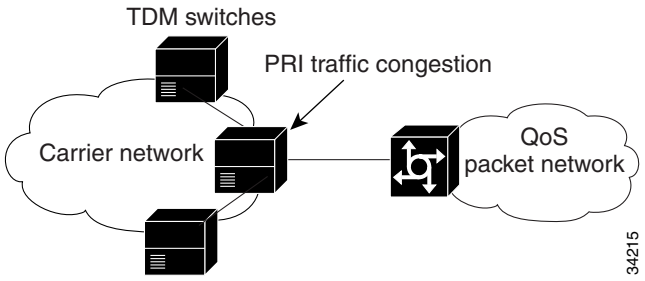
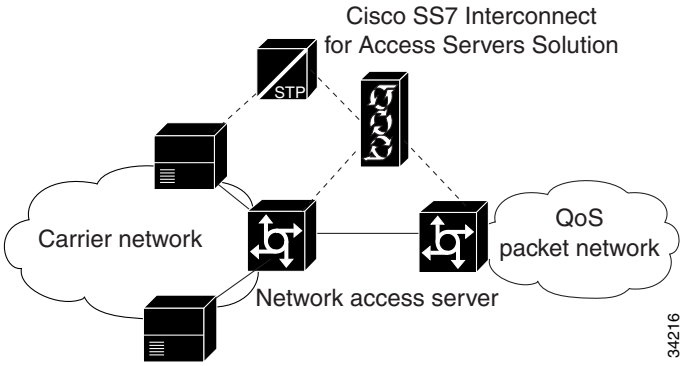


Figure 1-2 illustrates where the Cisco SS7 Interconnect for Access Servers Solution is located when it is dropped into a PSTN to offload calls. Note that the NASs are connected with a Cisco SC2200. By placing the Cisco SS7 Interconnect for Access Servers Solution as close to the ingress switch as possible, data traffic ties up fewer PSTN resources. The direct connection of the Cisco SS7 Interconnect for Access Servers Solution to the SS7 network provides advantages such as faster call setups and teardowns, as well as SS7's look-ahead capabilities for rerouting to avoid downed network nodes and links.

Figure 1-2 With the Cisco SS7 Interconnect for Access Servers Solution



Cisco Signaling Controller Product Information

The Cisco SC2200 is a signaling controller (SC) that converts telephony signals from one format to another. For example, the Cisco SC2200 converts SS7 signaling information from the PSTN to the signaling format required to establish calls between the PSTN and a packet data network.

The Cisco SC2200 is part of the Cisco Media Gateway Controller (MGC) product line. The Cisco MGC product line consists of hardware and software packages that you can use to connect your packet data network to the PSTN. Cisco MGC products manage call signaling conversion between the PSTN and the packet data network, and depending on the product, Cisco MGC products can control the routing of calls across the PSTN or packet data network.

Note Your Cisco SS7 Interconnect for Access Servers Solution documentation suite includes Cisco MGC reference books.

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

Understanding Terminology

The following key terms are used in this document to describe the Cisco SS7 Interconnect for Access Servers Solution architecture:

- Cisco SC2200—A hardware and software package that provides the signaling controller function. Typically this includes two SC hosts in a redundant configuration for continuous-service.
- SC host—A Sun host that runs 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 NASs that are provided with signaling services.

Architecture

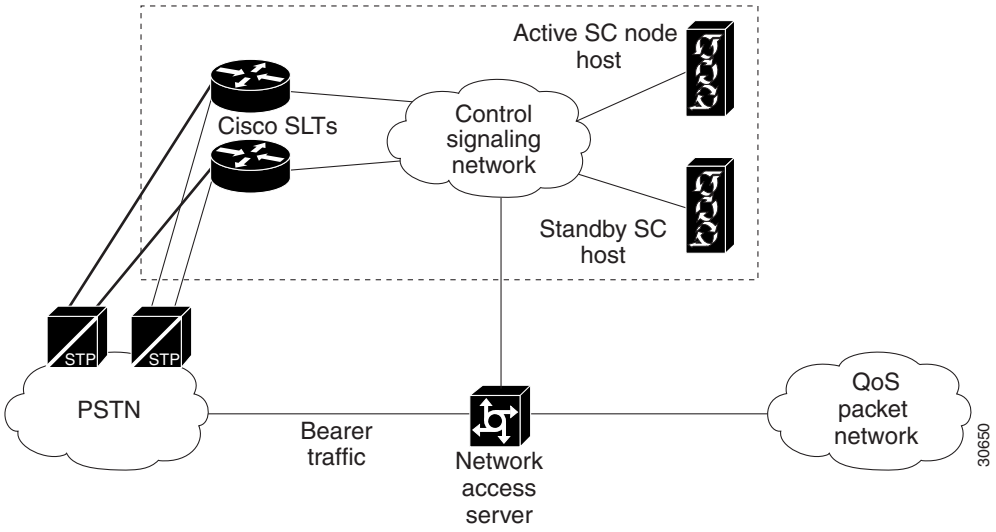
The architecture of the Cisco SS7 Interconnect for Access Servers Solution, shown in Figure 1-3, enables a NAS to operate in an environment where SS7 is used to establish calls on the bearer channels connected to the NAS.

Table 1-1 lists the components required by the Cisco SS7 Interconnect for Access Servers Solution. These components are described in greater detail in the "Cisco SS7 Interconnect for Access Servers Solution Components" section on page 2-7.

Table 1-1 Components for the Cisco SS7 Interconnect for Access Servers Solution

Component	Description
Cisco Signaling Controller Host (Cisco SC2200)	At MTP3 and higher layers, operates as an SS7 to ISDN protocol converter front-end to the NASs.
Cisco Signaling Link Terminal (Cisco SLT)	Used for physical SS7 link termination and MTP1 and MTP2 termination. **Note** The Cisco SLT is designed to be colocated with the Cisco SC2200 and interconnected with a local area IP network. Remote connectivity between the Cisco SLT and the Cisco SC2200 is currently not supported.
Cisco Network Access Server (Cisco AS5200, Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5800)	Used for data ISDN User Part (ISUP) trunk termination. **Note** The Cisco AS5200 can no longer be ordered. Cisco supports the existing installation base only.
LAN Switch (Cisco Catalyst Switch Family)	Provides infrastructure for the redundant and reliable Cisco SC2200 architecture. Connects multiple Cisco SLTs to the active and standby hosts within the Cisco SC2200 node. Connects the NASs with their controlling Cisco SC2200 node. Connects the originating Cisco SC2200 zone to the terminating Cisco SC2200 node between Cisco SC2200 zones. **Note** The switch is customer premises equipment and is not provided with the Cisco SC2200.
Cisco Media Gateway Controller Node Manager (CMNM)	Integrates the management interfaces and management functionality of the Cisco MGC node components into a comprehensive human interface and data repository. **Note** CMNM is available with Release 2.2 of the Cisco SS7 Interconnect for Access Servers Solution.

Figure 1-3 Cisco SS7 Interconnect for Access Servers Architecture



Benefits

Using the Cisco SS7 Interconnect for Access Servers Solution provides the following benefits:

- Provides wholesale dial services, dialup Virtual Private Networks (VPNs), Internet access, and voice services, while interconnecting as a carrier.
- Addresses voice network congestion by using the SS7 interfaces to make features such as rerouting on overflow conditions and the use of Intelligent Network (IN) functions possible, which further drives down operating costs.
- Replaces ISDN PRIs with bearer trunks and separates the signaling to increase bandwidth.
- Installs an SS7 POP in a new location without the added expense of a switch.
- Integrates the NASs directly into the SS7 network, using the Cisco SS7 Interconnect for Access Servers Solution and thus removes 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 E1/T1 software on the Cisco SLT.
- Transparently passes individual and uncompressed T1 or E1 channels between T1 or E1 ports by using Drop and Insert interfaces.

Features

Table 1-2 briefly lists features that are provided with your Cisco SS7 Interconnect for Access Servers Solution. For an overview of scalability and performance, system redundancy, management, and software requirements, see subsequent sections of this document. For the most up-to-date list of the supported telephony protocols, refer to the *Release Notes for Cisco Media Gateway Controller Software Release 7*.

Table 1-2 Features for the Cisco SS7 Interconnect for Access Servers Solution

Feature	Purpose
Directly connects access servers to PSTN in a peer-to-peer interconnect	• Reduces network costs. • Interconnects with more favorable tariffs and rates.
Intelligent Network (IN) triggers	• TCAP over IP. • TCAP local number portability (LNP) support. • 800/900 number translation.
Provides a reliable IP link between signaling controllers and NASs with Redundant Link Manager (RLM)	No single point of failure in connection between NAS and signaling controller.
Dial outsourcing	The Cisco SC2200 and NASs can be provisioned by telephone service providers and local exchange carriers. Calls can be directed to NASs belonging to various ISPs.
Facility-associated signaling provided by the Cisco SLTs	• Grooms off the bearer channels and then delivers them to the NASs. • Delivers MTP-3 to the signaling controller over Reliable User Data Protocol (RUDP).
Resource management	• Shares modems across POPs among various wholesale customers. • Single point of management.
Introduces services such as wholesale dial, Virtual Private Dial-up Networks (VPDNs), and virtual modem pooling	• Realizes new revenues. • Reduces PSTN congestion.
Supports colocated and distributed access servers	• Cost savings; scalable and flexible.
Supports Cisco AS5200, Cisco AS5300, Cisco AS5350, Cisco 5400, and Cisco AS5800 **Note** The Cisco AS5200 can no longer be ordered. Cisco supports the existing installation base only.	Investment in Cisco equipment protected.
Terminates and originates switching-system functions	• Enables new services. • Fast time to market. • Dial-out and dial-in. • Meets interconnect requirements.
Provides software upgrade of: • Cisco IOS software • MICA portware • Cisco SC2200 and Sun OS • Cisco SLTs	• Protects investments. • Provides low-cost ownership. • Is part of a complete solution with Cisco IOS software.

Table 1-2 Features for the Cisco SS7 Interconnect for Access Servers Solution (continued)

Feature	Purpose
• VPDN with Layer2 Forwarding (L2F) and Layer 2 Tunneling Protocol (L2TP) • Dial-out for callback and dial-on-demand routing (DDR) • Current remote access servers data features	• New revenue opportunities. • Complete services. • Investment protection.
• Radius or TACACS+ AAA functions, including authentication based on calling or called number • Call detail records for PSTN billing • Radius Proxy (GRS)	Meet PSTN requirements to create new service opportunities.
• SGCP 1.1+	Provides the general Internet Engineering Task Force (IETF) gateway control protocol function and the connection management statistics at the end of each connection in the call termination CDR. See the "Cisco Gateway Control Protocol Design" section on page 1-11 for details on SGCP 1.1+.
• SS7 protocols	Support the International Telecommunication Union Telecommunication Standardization Sector (ITU-T) SS7 protocol and many regional or national variants. For the most up-to-date list of the supported SS7 protocols, refer to the *Release Notes for Cisco Media Gateway Controller Software Release 7*.

Scalability and Performance

The Cisco SS7 Interconnect for Access Servers Solution includes the following scalability and performance features:

- Support for up to 50,000 DS0 ports
- Support for 250+ destination point codes (DPCs)
- Support for 6 originating point codes (OPCs)
- Support for up to 1500 simultaneous ISDN D-channels.
- Support for up to 32 signaling links
- Support for quasi-associated or fully associated signaling
- Complete continuity check (two-wire and four-wire)
- Compliance with NEBS Level 3 standards

System Redundancy

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

- Deploying the Cisco SS7 Interconnect for Access Servers Solution continuous-service configuration at your site. The continuous-service configuration consists of an active server and a standby server, linked with one another 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 the following features:
  - 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 SC2200. The links should be split across separate T1/E1 interface cards on the Cisco SLTs.

Cisco Signaling Controller Management

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

Table 1-3 Management Components of the Cisco Signaling Controller

Management Component	Description
Configuration Management	The Cisco MGC Manager (CMM) is a graphical user interface (GUI) that uses SNMP to configure and provision your Cisco SC2200. You can access the CMM remotely, using X terminals, and manage all the signaling controllers in your network with a single CMM system. Dial Provisioning Plan (DPP) is used to format the dial plan and routing data 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. The Cisco SC2200 is Simple Network Management Protocol (SNMP) capable, and MIBs are available.

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

Management Component	Description
Performance Management	You can get a variety of usage statistics from the signaling controller. The data is recorded realtime 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. The signalling controller is SNMP capable, and MIBs are available. Each performance measurement record includes: • Start time • Duration (START–STOP) • Measured value • Category • Element measured
Accounting Management	Every call that passes through the signaling controller produces call detail records (CDRs), which include: • CLI pretranslated • CLI posttranslated • Dialed number pretranslated • Dialed number posttranslated • Start, seizure, supervision, and disconnect time stamps • Call duration • Circuit path information CDRs 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.

Network Access Server Management

The Cisco IOS software installed on the NASs provides an array of network management components (described in Table 1-4). These management features do the following:

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

Cisco 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	The NASs are fully manageable by using the SNMP and embedded Remote Monitoring (RMON) capabilities: • SNMP provides for the collection of information about each server, 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 NASs both support CLI and the CiscoView graphical user interface (GUI) for comprehensive, flexible network management. CiscoView provides dynamic status, statistics, and comprehensive configuration information for Cisco switches, routers, NASs, Cisco SLTs, concentrators, and adapters. It displays a graphical view of Cisco devices, provides configuring and monitoring functions, and offers basic troubleshooting.
Modem Management	Modem management offers 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 the Cisco SLT and the Cisco SC host.

The Session Manager:

- Maintains separate communication sessions with each SC host in the pair.
- Uses RUDP to communicate between the Cisco SLT and the SC host.
- Handles the additional, fail-over traffic if a single Cisco SLT fails in a continuous-service configuration.

Note The Cisco SLT is designed to be colocated with the Cisco SC2200 and interconnected with a local IP network. Remote connectivity between the Cisco SLT and Cisco SC2200 is not currently supported.

Cisco Media Gateway Controller Node Manager

CMNM provides the element-specific management features for the Cisco MGC 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.

The key features of CMNM are:

- Performance monitoring
- Fault management
- Security
- Configuration
- Troubleshooting

Cisco Gateway Control Protocol Design

Starting with Release 2.2, the Cisco SC2200 platform simultaneously supports the following versions of the IETF gateway control protocols:

- SGCP 1.0: For details, refer to *Media Gateway Control Protocol for the Cisco AS5300 Voice/Gateway.* Available with the Cisco SC2200 Release 2.1 and earlier.
- SGCP 1.1+: This Cisco-proprietary extension of SGCP 1.1 includes the management of connections to the NASs, the parsing and building of messages, the tracking of network connection addresses, timers and retries. The protocol also supports the same set of CLI command verbs and parameters as supported in MGCP 0.1. Available with the Cisco SC2200 Release 2.2 and later.
- MGCP 0.1: For details, refer to *Media Gateway Control Protocol for the Cisco AS5300 Voice/Gateway.* Available with the Cisco SC2200 Release 2.2 and later.

The primary differences between SGCP 1.1+ and MGCP 0.1 are as follows:

- The two protocols use different protocol IDs.
- SGCP 1.1+ does not support the audit endpoint (AUEP) command to determine if connections exist for a given endpoint as supported by MGCP 0.1. Note that in SGCP 1.1+, the AUEP command is only used for the heartbeat function. To determine active connections for endpoints in SGCP 1.1+, the Cisco SC2200 uses SGCP 1.1+ DLCX message instead.

Note All three protocols are set, by default, to use the same UDP port. If your Cisco SC2200 platform is simultaneously supporting any of these protocol combinations: SGCP 1.0 and SGCP 1.1+; SGCP 1.0 and MGCP 0.1; or, SGCP 1.0, MGCP 0.1 and SGCP 1.1+, only SGCP 1.0 and MGCP 0.1 can be supported on the same UDP port. You need to change the default UDP port setting for SGCP1.1+ as it cannot use the same UDP port as SGCP 1.0 and MGCP 0.1.

The connection management statistics collected using the SGCP 1.1+ and MGCP 0.1 protocols are presented in the CDB TLV (Time, Length, Value) data elements. Table 1-6 summarizes the symbols used in those data elements:

Table 1-5 CDB Symbols and Descriptions

Symbol	Description
PS	Total packets sent by the gateway
PR	Total packets received by the gateway
OS	Octets sent by the gateway
OR	Octets received by the gateway
PL	Total packets lost by the gateway
JI	Jitter (average interpacket arrival jitter)
LA	Average latency
Rsrvd1	Reserved for future QoS information
Rsrvd2	Reserved for future QoS information

CHAPTER 2

Cisco SS7 Interconnect for Access Servers Configuration Options and Components

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

- Cisco SS7 Interconnect for Access Servers Solution Configurations
- Cisco SS7 Interconnect for Access Servers Solution Components

Cisco SS7 Interconnect for Access Servers Solution Configurations

The Cisco SS7 Interconnect for Access Servers Solution provides the following configuration options:

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

Simplex and Redundancy Options

You can deploy the Cisco SS7 Interconnect for Access Servers Solution in one of three ways:

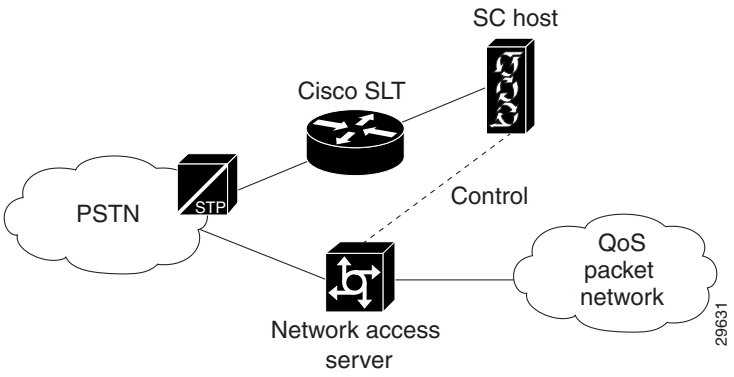
- Simplex Configuration
- Fault-Tolerant Configuration
- Continuous-Service Configuration

Simplex Configuration

A simplex configuration is an SC node that consists of a single SC host (Sun Netra t 112x) 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 network access servers provide bearer channel termination. See Figure 2-1.

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



Fault-Tolerant Configuration

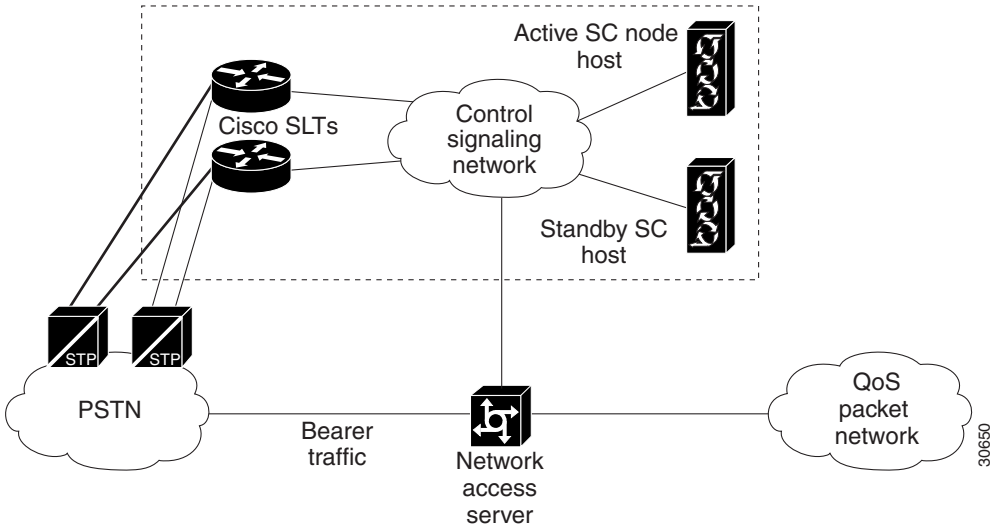
A fault-tolerant configuration is similar to a simplex configuration; however, the SC host must be a Sun Netra t 1400 server, a platform with redundant components. If a redundant component fails, the backup component takes over; established calls are maintained.

Continuous-Service Configuration

A continuous-service configuration is an SC zone that consists of a pair of SC hosts running in active mode and standby mode, operating with one or more network access servers and two or more Cisco SLTs. A heartbeat function runs continuously between the two SC hosts. 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 becomes the primary host, and 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 NAS.

Figure 2-2 Continuous-Service Configuration Example



Signaling Network Connections

The Cisco SS7 Interconnect for Access Servers Solution exchanges telephone control messages among the following components:

Cisco Signaling Controller—Provides signaling protocol conversion and Q.931 call control to communicate with the NASs. One signaling controller might provide signaling and call-processing services for multiple NASs in geographically distributed locations.

Cisco SLT—Handles incoming and outgoing SS7 messages (MTP layer 1 and 2) from the A-links connected to Signal Transfer Points (STPs) or F-links connected to other 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 sends the bearer channels to the NAS.

Cisco Network Access Server—Provides termination for bearer trunks. A NAS functions as a server to the bearer links. The NAS has at least two IP network interfaces: one to carry IP packet data onto one or more backbones and another to connect to the ISP's secure management, signaling, and Q.931 control network.

Your Cisco SS7 Interconnect for Access Servers Solution can be deployed with the following SS7 signaling network connections:

- 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

In the A-link SLT signaling configuration, the Cisco SLT processes the two lowest-layer SS7 signaling protocols, MTP1 and MTP2. The upper layer protocols are then forwarded to the Cisco MGC host over the control signaling network. Each SLT supports two signaling network connections, and multiple SLTs can be used to support additional signaling channels or provide redundant signal paths between the signaling network and the control signaling network.

The A-link SLT signaling configuration supports V.35, T1, and E1 interfaces. The A-link SLT configuration can be used with simplex and continuous-service configurations. Each interface supports a single DS0 signaling channel.

F-Link with Cisco SLT

F-link SLT signaling configurations are similar to A-link SLT configurations. The SS7 network connection is made through fully associated links that connect an SSP or SCP to the Cisco SLT.

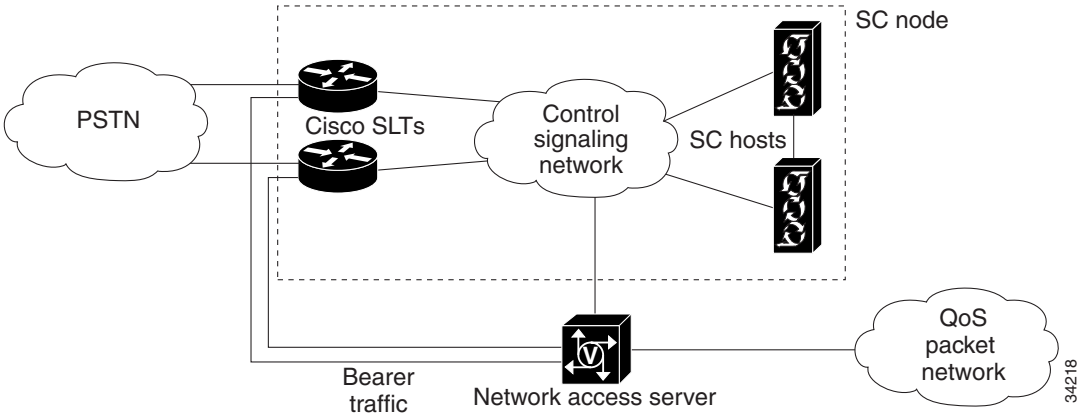
The F-link SLT signaling configuration supports V.35, T1, and E1 interfaces. The F-link SLT configuration can be used with simplex and continuous-service host configurations. Each interface supports a single DS0 signaling channel.

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 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 2-3.

Note The A-Link and F-link Drop and Insert techniques are also known as time-division multiplexing (TDM) cross-connect.

Figure 2-3 F-Link Drop and Insert Configuration



The F-link drop and insert signaling configuration supports T1 and E1 interfaces. The Drop and Insert cards are special two-port cards designed for this application and installed in the Cisco SLT. Signal and bearer traffic enter one port together. The Cisco SLT grooms the bearer traffic and then 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 Access Servers 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 (Redundant Link Manager (RLM) with the required SC host and NAS, Cisco SLT redundancy, and timers)

Control traffic (signaling) should be segregated from the bearer traffic on the QoS packet network (towards the Internet/intranet). This optimizes control traffic latency and provides added security. Redundancy in your control network can be provided by duplicating your Cisco SS7 Interconnect for Access Servers Solution components. In the event that the control network fails or connectivity to it fails, the QoS packet network is used for signaling.

In the simplest case, your Cisco SS7 Interconnect for Access Servers Solution components are co-located, and a pair of LAN switches serves as your control network. Cisco Systems recommends that the Cisco SLT not be deployed remotely from the Cisco SC2200. Remote configurations include, but are not limited to, those based on dedicated ATM connections or other similar dedicated facilities. Installing the Cisco SLT remotely from the Cisco SC2200 compromises the SS7 link stability and can eventually cause the SS7 link to fail during high traffic.

IP Connectivity with LAN

Figure 2-2 shows a sample continuous-service 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-service configuration example, the control signaling network functions are:

- Checkpointing traffic (RUDP/UDP/IP)
- Heartbeat (UDP; 50 bytes/sec)
- SNMP management of components
- SC/Cisco NAS signaling and communications (Q.931+/Q921/UDP/IP-RLM)
- SC/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

- Network access server/RPMS traffic
- Network access server/AAA (RADIUS/TACACS+server traffic)

IP Connectivity with WAN

Distributed IP control networks operating over a WAN is necessary when:

- Multiple POPs in geographically different locations are controlled by the same SC host.
- Redundant SC hosts are in geographically different locations.

Note The NAS is equipped with serial ports providing WAN termination.

IP Control Network Combinations

The following IP control network combinations are recommended:

- One single subnet for all traffic.
- Two redundant subnets: one for 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 NAS/SC host traffic. Note: one of these subnet pairs must also run user data traffic.
- Any combination of the above with WAN links and dedicated routers providing IP connectivity between the SC host/NAS subnets and the SC host subnet.
- 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:

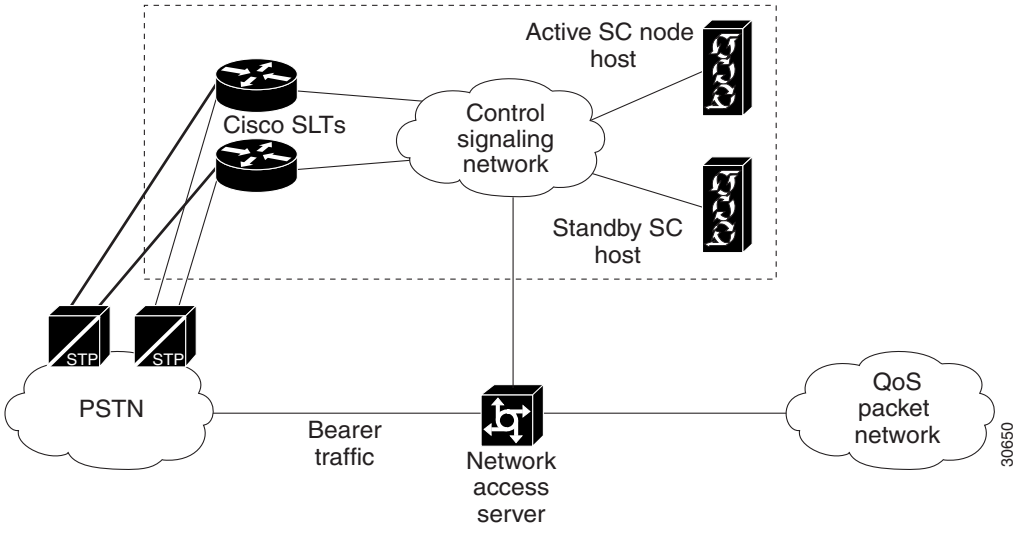
- There should be no packet loss, and the packets should not be received out of order between the signaling controller and the NASs. This could impact the performance of the Cisco SS7 Interconnect for Access Servers Solution, causing call setup time to reach unacceptable levels.
- Do not enable load balancing in the control network. If you must use load balancing, then 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 NASs 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 Access Servers Solution Components

Figure 2-4 shows the components of the Cisco SS7 Interconnect for Access Servers Solution.

See the "SS7 Technology Overview" appendix for information about how the Cisco SS7 Interconnect for Access Servers Solution components operate within the SS7 hierarchy.

Figure 2-4 Cisco SS7 Interconnect for Access Servers 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 Access Servers Solution consists of one or more SC hosts, one or more Cisco SLTs, the signaling controller software, and ancillary equipment.

This section describes the SC hosts, signaling and Ethernet interface options, and the ancillary hardware requirements. For details on software requirements, refer to the *Cisco SS7 Interconnect for Access Servers Upgrade Guide* at the following location:

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

SC Hosts

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 Ultra Enterprise 450 (E450)	The Sun Ultra Enterprise 450 is a high-performance, shared-memory, multiprocessing, general-purpose Sun Ultra SPARC server. **Note** The Sun E450 is not NEBS compliant. **Note** The Sun E450 can no longer be ordered. Cisco supports the existing installation base only.
Sun Netra t 1120/1125	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. The Sun Netra 1120 uses DC power and the Sun Netra 1125 uses AC power.
Sun Netra t 1400	The Sun Netra t 1400 is a fault-tolerant, dual modular, redundant architecture. Additional lockstep operations give this host the ability to isolate and recover from hardware failure. The Sun Netra t 1400 is NEBS and ETSI compliant.
Sun Netra ft 1800	The Sun Netra ft 1800 is a fault-tolerant, dual modular, redundant system with the Overriding Principle design. Overriding Principle means that no single point of failure will occur, and all active modules can be removed and replaced online. The Sun Netra ft 1800 is ETSI compliant and is fully certified to level 3 of the NEBS standard.

SC Host Features

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

- Interworking a variety of 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
- 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 host.

Table 2-2 SC Host Features

Feature	Support for ...
Call performance per signaling controller	• As many as 100 calls per second with 30 K to 50 K simultaneous calls • As many as 200 calls per second with 100,000 simultaneous calls and with Cisco SC2200 call-processing software optimization
Management interfaces	• 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
Faults and alarms management	SNMP traps
Millisecond time stamp	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".
Logging enhancements for Release 2.2	Improved system logging efficiency and ability to diagnose problems. The logging utility is enhanced in the following areas: • Enhanced log format: consistent, text-based message logs and separate logs for the system and users. • Improved system efficiency: dynamic and non-service- interrupting filtering capabilities for specific logging. • Improved user efficiency: ability to work with other tools (for example, grep utility) and improved log reliability.
Configuration management	• Cisco MGC Manager (CMM), a TCL/tk graphic user interface (GUI) that uses simple network management protocol (SNMP) commands to provision the SC host. • Man-Machine Language (MML), a command-line interface to the SC host.
Accounting	CDR (CSV format) support for international carrier requirements
Resource management	• Keeps track of circuit IDs for assigning calls on NAS ports • Manages adds, moves, and changes of NAS resources
Performance measurements and statistics	Supports carrier requirements
Security	Structured system of passwords

Table 2-2 SC Host Features (continued)

Feature	Support for ...
Operating system	Sun Solaris 2.6.x
Dial Plan Provisioning Enhancements	Enables you to input the 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.
MML-control of call processing resources	Provides a MML command interface to allow or reject any new calls.
Route List Display	Displays the symbolic name of a route list in the Telephony Controller Manager (TCM).
Configuration Upload/Download	Provides 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	Displays component IDs in terms of MML names in system logs.
Bearer Channel Level Tracing	Provides a call tracing capability through the MML interface to generate machine-readable traces to be used by Call Trace Viewer (CTV) applications.
Viewer Tools	Provides 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 dial plan.
Memory Reduction	Provides a per-call, post-answer memory reduction mechanism to accommodate 100,000 simultaneous calls on the 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.
Scalable D-channel connection	Provides enhanced SC host infrastructure to support as many as 1500 simultaneous D-channel connections.

Signaling and Ethernet Interface Options

Table 2-3 shows the signaling and Ethernet interface options for the Cisco SC2200.

Table 2-3 SC Signaling and Ethernet Interface Options

Interface Option	Sun Netra t 1120	Sun Netra t 1400	Sun Netra ft 1800	Sun E450[1]
ITK T1/E1 card	Supported	Not supported	Not supported	Supported
PTI V3.5 card	Supported	Not supported	Not supported	Supported
Sun Ethernet 1-port card	Required	Required	Not supported	Required
Cisco SLT	Supported	Supported	Supported	Supported

1. Starting with Release 2.1, Sun E450 can no longer be ordered. Cisco supports the existing installation base only.

Note Cisco recommends that you upgrade to the Cisco SLT to terminate the telephony signaling links. Starting with Release 2.1, ITK T1/E1 and PTI V.35 cards can no longer be ordered. Cisco supports the existing installation base only.

Ancillary Hardware Requirements

Table 2-4 shows the ancillary hardware requirements for the Cisco SC2200.

Table 2-4 SC Ancillary Hardware Requirements

Component	Sun Netra t 1120	Sun Netra t 1400	Sun Netra ft 1800	Sun E450[1]
Dataprobe Alarm Relay Unit (ARU)	Supported[2]	Not supported	Not supported	Supported and required only for alarm functions
Dataprobe A/B Switch	Required with use of ITK T1/E1 or PTI V.35 cards[3]	Not supported	Not supported	Required with use of ITK T1/E1 or PTI V.35 cards[3]
Asynch Extension	Optional for simplex configurations; required with use of Dataprobe A/B switch	Not supported	Not supported	Optional for simplex configurations; required with use of Dataprobe A/B switch

1. Starting with Release 2.1, Sun E450 can no longer be ordered. Cisco supports the existing installation base only.
2. Cisco does not recommend using Dataprobe ARU. You should use the built-in alarm card and software.
3. Call preservation upon switchover or failover is not supported with the A/B switch.

Cisco SLTs

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 2-5 lists the features for the Cisco SLT.

Table 2-5 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 Cisco 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, V.35, RS-449, and RS-530.
Drop and Insert	Cisco T1/E1 Multiflex Voice/WAN interface cards (VWICs) support Drop and Insert (also called TDM Cross-Connect), which allows individual T1/E1 channels to be transparently passed, uncompressed, between T1/E1 ports. This feature enables direct termination of SS7 F-links in T1 or E1 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 2-6 lists the features of CMNM.

Table 2-6 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 2-6 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

Network Access Servers

The NAS terminates the PSTN trunks, also referred to as bearer channels, that carry the call traffic. The PSTN trunks are T1 or E1 PRI interfaces.

Note Cisco IOS Release 12.1(3) or later releases run on the NAS.

Table 2-7 lists the features for the Cisco AS5*x*00 series.

Table 2-7 Cisco AS5x00 Features

Feature	Support for...
Continuity testing	Automated diagnostic procedure.
Redundant Link Manager	Virtual link management.
Resource Pool Management	Shared dial resources for wholesale and retail dial network services on a single NAS.
Resource Pool Management Server	Shared dial resources for wholesale and retail dial network services across multiple NAS stacks.

LAN Switches (Optional)

The control signaling network for the Cisco SS7 Interconnect for Access Servers Solution often consists of a LAN switch and the cabling required to interconnect the solution components in an SC zone. The Cisco SS7 Interconnect for Access Servers 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

Cisco SS7 Interconnect for Access Servers Solution Operations

This chapter provides a brief overview of unattended operations and manual control options available on your Cisco SS7 Interconnect for Access Servers Solution.

Unattended Operation

The following operations are described in this section:

- Understanding System Redundancy
- Understanding Automatic Switchover
- System Messages
- Call Detail Records
- Disk Mirroring

Understanding System Redundancy

The Cisco SS7 Dial Access Solution uses two SC hosts with software-based checkpointing and heartbeat to facilitate redundancy. The call-processing application is active only on 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 host to switch traffic to the now active SC host. Upon switchover, all calls answered in progress are preserved.

Note Full system redundancy is available only on continuous service configurations.

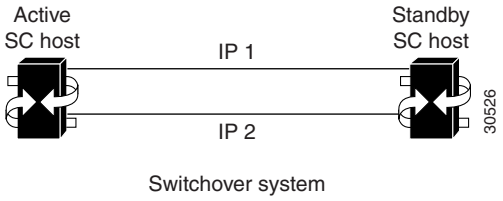
Understanding Automatic Switchover

The Cisco SS7 Dial Access Solution offers the continuous service configuration to protect your system against failures and downtime. A feature enhancement to Redundant Link Manager (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 (either dual Sun E450s or Sun Netras) 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 outputs 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 signal controller software, formats the messages, and outputs 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 the *Cisco Media Gateway Controller Software Release 7 Reference Guide* at the following location:

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

Call Detail Records

CDRs comprise 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 a result of Cisco signaling controller system enhancements. For detailed information about CDEs and CDBs and an overview of the Cisco Signaling Controller billing system, see these Cisco SS7 Interconnect for Access Servers Solution documents:

- *Cisco Media Gateway Controller Software Release 7 Operations, Maintenance, and Troubleshooting Guide* at the following location:

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

- Cisco *Media Gateway Controller Software Release 7 Installation and Configuration Guide* at the following location:

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

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 1400 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 on page 3-1.

The Sun 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* at the following location:

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

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 MGG 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 Provisioning Guide* at the following location:

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

Although MML provisioning requires more keystrokes, quick provisioning updates can sometimes be made faster with MML commands, because you don't have to go through the process of launching CMM. When you enter MML commands into a batch file, you can copy and paste configuration commands to speed command entry, and you can copy and modify MML scripts to configure additional Cisco MGC switches. For information on provisioning with MML, see the *Cisco Media Gateway Controller Software Release 7 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 TCM 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 Sun Solaris 2.6 OS Running the CMM 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

Cisco SS7 Interconnect for Access Servers Solution Implementation

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

Implementation Task List

To implement your Cisco SS7 Interconnect for Access Servers 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:

a. Signaling routes to external switches

b. Signaling links to signaling points

c. Network access server control links

d. 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 Cisco 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 Cisco SC 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 IP addresses 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 network access server. See the "Network Access Server Installation and Configuration" section for details.

- **a.** Connect the network access server to the LAN switch.
- **b.** Connect the network access server to the Public Switched Telephone Network (PSTN).
- **c.** Configure and assign IP addresses to the network access servers. See the section "Network Access Server Installation and Configuration" for details.

Step 10 Configure the network management server. See the "Operation and Maintenance" section for details.

Step 11 Make sure that all the devices can talk to each other by pinging one device from another.

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 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 network access servers will be connected.	

Cisco SLT Installation

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

Note Cisco Systems recommends that the Cisco SLT not be deployed in a remote configuration from the Cisco SC2200. Remote configurations include, but are not limited to, configurations based on dedicated ATM connections or other similar dedicated facilities. Installing the Cisco SLT remotely from the Cisco SC2200 compromises SS7 link stability and can eventually cause the SS7 link to fail during high traffic.:

	Task	Reference
Step 1	Connect serial ports through the T1/E1, V.35, RS-449, or RS-530 interfaces to the STPs.	• *Cisco Media Gateway Controller Hardware Installation Guide* • Cisco IOS Release 12.0(7)XR documentation, *Cisco Signaling Link Terminal*
Step 2	Connect Ethernet ports through the Ethernet 10BaseT 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 network access servers to the LAN switch. If you have two IP networks, use the network access server Ethernet port to connect each network access server to the POP management network, and use the network access server Fast Ethernet port to connect each network access server to the IP data network.	• *Cisco Media Gateway Controller Hardware Installation Guide*
Step 2	Connect the bearer channels to the network access server using RJ-48 connections for the E1 and T1 interfaces.	

Signaling Controller Software Installation

This section provides an overview of the recommended software installation sequence. For details, refer to the appropriate software installation guide.

	Task	Reference
Step 1	Install the operating system on the signaling controller: 1. Verify SC host firmware. 2. Install the Sun Solaris operating system. 3. Install the Volume Manager. 4. 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: 1. Install the software for a single-host or dual-host configuration. 2. Configure the execution environment. 3. Terminate the signaling links. 4. Configure the SNMP support resources.	
Step 3	Install IOS Release software 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 signaling controller TCM tool or MML commands to create, modify, manage, and deploy your configuration files on the signaling controller. We do 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 Guide*

	Task	Reference
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 SS7network (through the Cisco SLT).	
Step 4	Configure the network access server control links by completing the following tasks: • Add external nodes for the NASs in your network. • Add NAS signaling services for each NAS. • Add IP links for each NAS to each Ethernet card in the SC host.	
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 WAN Interface Cards Hardware Installation Guide*
- *Software Configuration Guide for Cisco 2600 and 3600 Series Routers*
- *New and Changed show Commands for Cisco 2600 Series Routers*
- *Cisco 2600 Series Configuration Notes*

Tips The Cisco publications are available online on the Cisco web site 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 network access servers or the Cisco Signaling Link Terminals (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 signaling controller. 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.	

Network Access Server Installation and Configuration

To install the network access server, perform the following tasks:

	Task	Reference
Step 1	Rack-mount the network access server chassis.	*Cisco SS7 Interconnect for Access Servers and Voice Gateways Solutions Media Gateway Guide*
Step 2	Connect the network access server 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 network access server.	

For each network access server installed in your Cisco SS7 Interconnect for Access Servers Solution, configure the network access server 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 network access server 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 or E1 lines.	
Step 3	Configure the D channels for modem signaling and receiving calls using the RLM-group command.	
Step 4	Set ISDN timers T309 and T321 to 0.	

To install the optional network access server software features supported on your Cisco SS7 Interconnect for Access Servers Solution, perform the following tasks:

	Task	Reference
Step 1	Configure Continuity Testing (COT)	Cisco IOS Release 12.0 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 documentation • *Cisco SS7 Dial Access Solution*
Step 3	Configure the Resource Pool Manager (RPM)	Cisco IOS Release 12.0 documentation • *Cisco SS7 Dial Access Solution*
Step 4	Configure the Resource Pool Management Server (RPSM)	Cisco IOS Release 12.0 documentation • *Cisco SS7 Dial Access Solution*

Operation and Maintenance

Under normal conditions, the primary (active) signaling controller application (which includes 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 (an answer message has been received). This ensures that the call state is maintained in case of failure.

The following are normal operating procedures for the signaling controller:

- Managing signaling channels and lines
- Managing traffic channels

- Managing switchover

The following are operating procedures under various equipment failure scenarios:

- Signaling link termination failure
- Signaling controller 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

Note For detailed instructions on these operation procedures and maintenance tasks, see the *Cisco Media Gateway Controller Release 7 Operations, Maintenance, and Troubleshooting Guide*.

You can also initiate your case online through the Internet at www.cisco.com. Outside these locations, contact the Cisco regional sales office nearest you, or contact your local authorized Cisco distributor.

Related Documentation

The following documentation related to the Cisco SS7 Interconnect for Access Servers Solution is available on CCO and elsewhere on the Internet:

- Cisco Media Gateway Controller Release 7 Documentation:
  http://www.cisco.com/univercd/cc/td/doc/product/access/sc/rel7/soln/index.htm
- *Cisco Dial Solutions Quick Start Guide*:
  http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/12supdoc/dsqcg3/index.htm
- *Cisco Dial Solutions Configuration Guide*:
  http://www.cisco.com/univercd/cc/td/doc/product/software/ios113ed/113ed_cr/dial_c/index.htm
- *Cisco Dial Solutions Command Reference*:
  http://www.cisco.com/univercd/cc/td/doc/product/software/ios113ed/113ed_cr/dial_r/index.htm
- Cisco SC2200 documentation, *Cisco SS7 Dial Access Solution System Integration Guidelines*:
  http://www.cisco.com/univercd/cc/td/doc/product/access/sc/r2/6011.htm

- Cisco Network Access Server configuration:

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios113ed/113aa/113aa_7/rlm_rel2.htm

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios113ed/113aa/113aa_5/cot.htm

  http://www.cisco.com/univercd/cc/td/doc/product/access/acs_serv/as5200/index.htm

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

  http://www.cisco.com/univercd/cc/td/doc/product/access/acs_serv/as5350/index.htm

  http://www.cisco.com/univercd/cc/td/doc/product/access/acs_serv/as5400/index.htm

  http://www.cisco.com/univercd/cc/td/doc/product/access/acs_serv/as5800/index.htm

  Note Cisco AS5200 access servers can no longer be ordered. Cisco supports the existing installation base only.

- Cisco Signaling Link Terminal:

  http://www.cisco.com/univercd/cc/td/doc/product/access/acs_mod/cis2600/ios_feat/0219nomd.htm

- Cisco Access Server documentation:

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

- Cisco AccessPath system documentation:

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

- Cisco Access Server Release Notes:

  For the Cisco AS5200:

  http://www.cisco.com/univercd/cc/td/doc/product/access/acs_serv/as5200/ios52/index.htm

  For the Cisco AS5300:

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

  For the Cisco AS5350

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121relnt/5350/rn5350xm.htm

  For the Cisco AS5400:

  http://www.cisco.com/univercd/cc/td/doc/product/access/acs_serv/as5400/ios_rn/index.htm

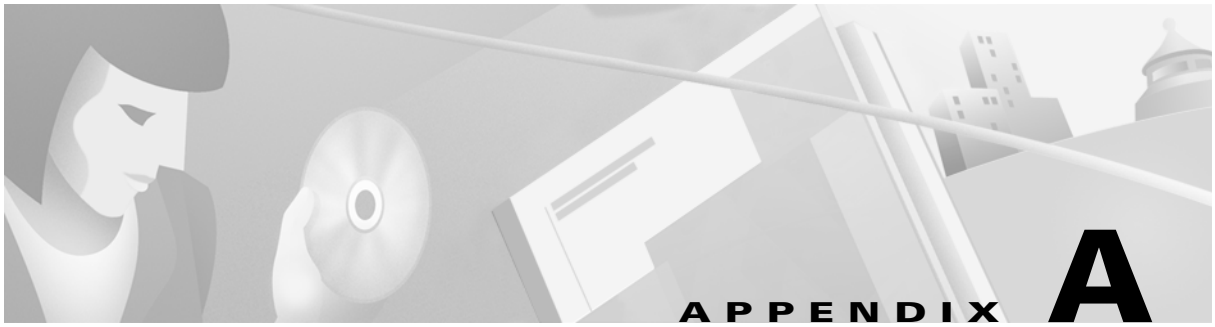
  For the Cisco AS5800:

  http://www.cisco.com/univercd/cc/td/doc/product/access/acs_serv/as5800/58_iosrn/index.htm

- SS7 tutorial:

  http://www.iec.org/

  Click Training, Web ProForum Tutorials, Communications Networks, and then scroll down the list and click Signaling System #7 (SS7).



APPENDIX A

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 that the term SS7 can be used to refer to the SS7 protocol, the signaling network, or the signaling network architecture.)

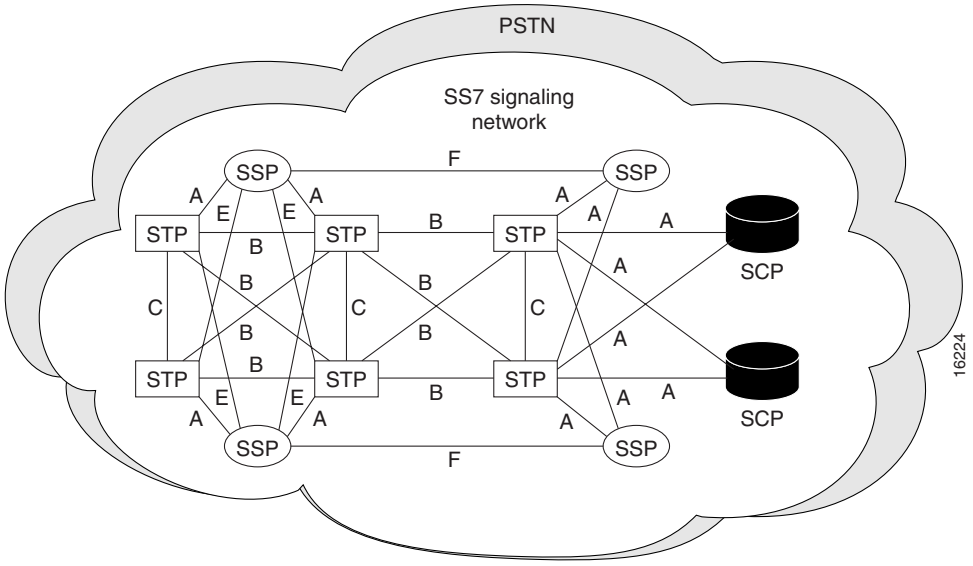
The SS7 protocols that convey signaling information between switching systems (called signaling points) in the PSTN are carried on a special overlay network used exclusively for signaling. The signaling points use routing information in the SS7 signals to transfer calls to their final destinations.

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

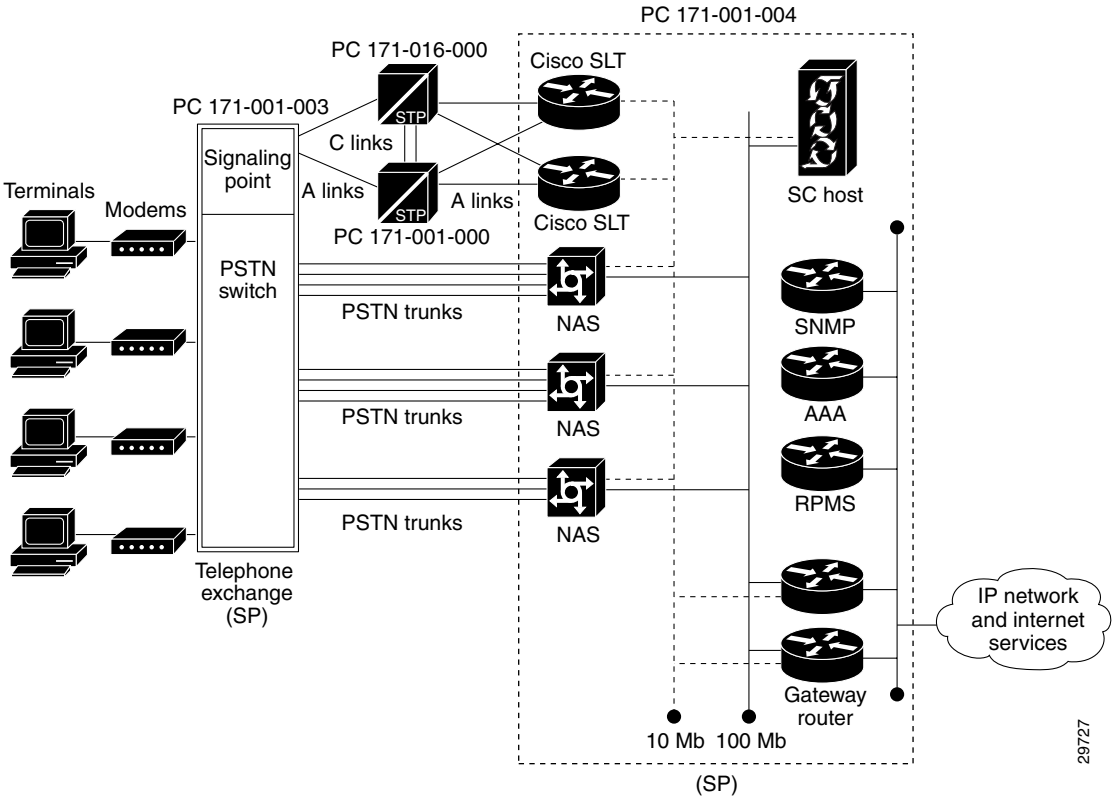
Each signaling point (also called an SS7 node or SP) in the SS7 network is identified with a unique address called a point code (PC). ANSI point codes are 24-bit and ITU point codes are 14-bit. PCs are carried in signaling messages exchanged between signaling points to identify the source and destination 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 PC 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 MGC signaling point.

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.
- Russel, T. Signaling System #7, McGraw Hill Telecommunications.
- http://www.iec.org/. Click **Training**, **Web ProForum Tutorials**, **Communications Networks**, and then scroll down the list and click **Signaling System #7 (SS7**).

A

B

C

D

E

F

G

H

I

L

M

N

O

P

R

S

T

U

W