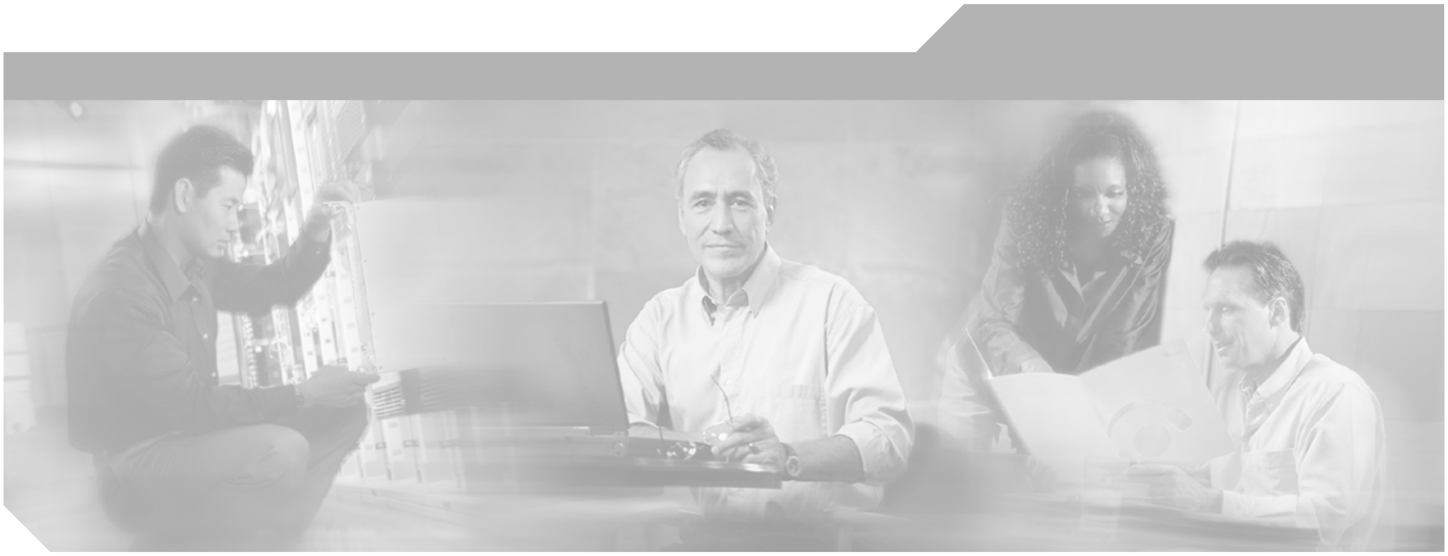


Cisco SS7 Interconnect for Access Servers and Voice Gateways Solutions Upgrade Guide

July 23, 2002

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: 78-10991-04

Cisco SS7 Interconnect for Access Servers and Voice Gateways Solutions Upgrade Guide

CONTENTS

CHAPTER 6

CHAPTER 7

Preface

This preface describes the objectives, audience, organization, and conventions of this document, and explains how to find additional information on related products and services. It contains the following sections:

- Document Objectives, page ix
- Audience, page x
- Document Organization, page xi
- Conventions, page xii
- Documentation Suite, page xiv
- Obtaining Documentation, page xvii
- Obtaining Technical Assistance, page xviii

Document Objectives

This guide contains procedures for upgrading within the Cisco SS7 Interconnect for Access Servers and Voice Gateways Solutions. These procedures describe how to upgrade the following releases:

- From an installed Cisco SS7 Dial Access Solution (DAS) Release 2.0 to the Cisco SS7 Interconnect for Access Servers Solution Release 2.1 or 2.2
- Within a Cisco SS7 Interconnect for Access Servers Solution, from Release 2.1 to Release 2.2
- Within a Cisco SS7 Interconnect for Voice Gateways Solution, from Release 1.0 or 1.1 to Release 1.3

The Cisco SS7 Interconnect for Access Servers Solution is the second version of Cisco's solution that provides dial offload services to IP networks. The first version was the Cisco SS7 DAS.

To follow the procedures in this manual, you should be familiar with the signaling controller (SC), Man-Machine Language (MML), the UNIX operating system, and Cisco IOS software.

Note This guide uses *SC host* to refer to the combinations of Sun Microsystems, Inc. server hardware and *SC software*. The SC software supports other network solutions (in addition to the signaling controller) and is also called the *Cisco Media Gateway Controller (MGC) Software*. The software is also called the *Cisco Telephony Controller Software.*

These procedures are designed for upgrading both simplex (single) and high-availability configurations that contain two signaling controllers to provide switchover functions. In a simplex system, all call processing stops if an SC host fails. In the high-availability configuration, one host (active) is paired with a backup host (standby) that is designed to automatically take over as the active host if failure in call processing occurs.

In the Cisco SS7 Interconnect for Access Servers Solution, Cisco Systems recommends that signaling links no longer terminate in the A/B switch and ITK cards on the SC host, but be connected to Cisco Signaling Link Terminals (SLTs). Using the Cisco SLTs to terminate signaling provides a more robust and fault-tolerant system. A configuration using two SC hosts and two Cisco SLTs is a continuous-service configuration. A configuration using two SC hosts and ITK cards to terminate signaling is a high-availability configuration.

Note The cards referred to as “ITK” are manufactured by Digi International AG (formerly known as IT Telekommunikations AG [ITK]).

Tip The latest version of this guide and other documents referred to in this guide are always found on Cisco.com. Make sure that you are using the latest version of the documents before beginning these procedures.

Audience

The primary audience for this document is network operators and administrators who have experience in the following areas:

- Telecommunications network operations
- Data network operations
- SS7 protocols, switching, and routing
- Telecommunications hardware
- Data network hardware

In addition, the following audiences may find this document useful:

- Software and hardware installers
- Network designers

Document Organization

The major sections of this guide are summarized in Table 1.

Table 1 Document Contents

Chapter	Title	Content
Chapter 1	Solution-Level Upgrade Procedures	Provides general information about upgrading your solution, including: • Tips for performing the upgrade • Hardware and software requirements • Procedural overview for each upgrade type
Chapter 2	Backing Up Your SC Host Data	Contains instructions for backing up your SC host data before performing the upgrade.
Chapter 3	Cisco Media Gateway Upgrade Procedures	Contains procedures for upgrading your Cisco 5x00 Access Servers.
Chapter 4	Cisco Signaling Link Terminal Upgrade Procedures	Contains procedures for upgrading your solution with the Cisco SLT and for upgrading the Cisco SLT itself.
Chapter 5	Upgrading SC Host Hardware	Provides hardware upgrade instructions for the Sun Netra t 100/105, Netra t 1120/1125, and Netra t 1400/1405. Covers upgrading the following components: • Hard drives • Processors • Memory
Chapter 6	Installing the Operating System on the SC Hosts	Contains instructions for installing the Sun Solaris 2.6 operating system and related software, including: • Solaris patches • Volume manager software • Alarm card software
Chapter 7	Upgrading Cisco SC2200 Software	Provides upgrade procedures for the Cisco SC2200 software. Includes directions for installing patches, restoring SC host configurations, and verifying proper functioning of the software.

Conventions

Table 2 provides descriptions of the conventions used in this document.

Table 2 Document Conventions

Convention	Description of usage	Comments
Boldface	Commands and keywords you enter literally as shown	**offset-list**
Italics	Variables for which you supply values	**command** *type interface* You replace the variable with the type of interface. In contexts that do not allow italics, such as online help, arguments are enclosed in angle brackets (< >).
Square brackets ([ ])	Optional elements	**command** [abc] abc is optional.
Vertical bars (l)	Separated alternative elements	**command** [abc l def] You can choose either abc or def, or neither, but not both.
Braces ({ })	Required choices	**command** { abc l def } You **must** use either abc **or** def, but not both.
Braces and vertical bars within square brackets ([{ l }])	A required choice within an optional element	**command** [abc { def l ghi }] You have three options: nothing, abc def, or abc ghi.
Caret character (^)	Control key	The key combinations ^D and Ctrl-D are equivalent: Both mean hold down the Control key while you press the D key. Keys are indicated in capital letters, but are not case-sensitive.
A string	A nonquoted set of characters	For example, when your are setting an SNMP community string to *public*, do not use quotation marks around the string; otherwise, the string will include the quotation marks.
`System prompts`	Denotes interactive sessions, indicates that the user enters commands at the prompt	The system prompt indicates the current command mode. For example, the prompt `Router (config) #` indicates global configuration mode.
`Screen` font	Terminal sessions and information the system displays	

Table 2 Document Conventions (continued)

Convention	Description of usage	Comments
Angle brackets (< >)	Nonprinting characters such as passwords	
Exclamation points (!) at the beginning of a line	A comment line	Comments are sometimes displayed by the Cisco IOS software.

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

Timesaver Means the *described action saves time*. You can save time by performing the action described in the paragraph.

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

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

Warning **This warning symbol means *danger*. You are in a situation that could cause bodily injury. Before you work on any equipment, you must be aware of the hazards involved with electrical circuitry and familiar with standard practices for preventing accidents. (To see translated versions of this warning, refer to the *Regulatory Compliance and Safety Information* that accompanied your equipment.)**

Table 3 describes the various data type conventions used in this document.

Table 3 Data Type Conventions

Data Type	Definition	Example
Integer	A series of decimal digits from the set of 0 through 9 that represents a positive integer. An integer might have one or more leading zero (0) digits padded on the left side to align the columns. Leading zeros are always valid as long as the number of digits is less than or equal to ten digits total. The range of values is 0 through 4294967295.	123 000123 4200000000
Signed integer	This data type has the same basic format as the integer but can be positive or negative. When negative, it is preceded by the minus sign (–) character. As with the integer data type, this can be as many as 10 digits in length, not including the sign character. The value of this type has a range of –2147483647 through 2147483647.	123 –000123 –2100000000l

Table 3 Data Type Conventions (continued)

Data Type	Definition	Example
Hexadecimal	A series of 16-based digits from the set of 0 to 9, a to f, or A to F. The hexadecimal number might have one or more 0 digits padded on the left side. For all hexadecimal values, the maximum size is 0xffffffff (8 hexadecimal digits).	1f3 01f3000
Text	A series of alphanumeric characters from the ASCII character set. Tab, space, and double quote (" ") characters cannot be used. Text can be as many as 255 characters; however, it is recommended that you limit the characters to no more than 32 for readability.	EntityID LineSES_Threshold99
String	A series of alphanumeric characters and white-space characters. A string is surrounded by double quotes on the left and right sides (" "). Text can be as many as 255 characters; however, it is recommended that you limit the characters to no more than 80 for readability.	"This is a descriptive string."
Note	Hexadecimal and integer fields in files might have different widths (number of characters) for column alignment.	
IP address	The standard TCP/IP address expressed as four numbers, where each number is from 0 through 255 and consecutive numbers are separated by a period.	139.85.60.17 or 127.55.13.200

Documentation Suite

Consult the following documents for information about the Cisco SS7 Interconnect for Access Servers and Voice Gateways Solutions.

- *Cisco SS7 Interconnect for Access Servers Solution Overview*
- *Cisco SS7 Interconnect for Voice Gateways Solution Overview*
- *Cisco SS7 Interconnect for Access Servers and Voice Gateways Solutions Gateway Guide*
- *Cisco SS7 Interconnect for Access Servers and Voice Gateways Solutions Provisioning Guide*
- *Cisco SS7 Interconnect for Voice Gateways Solution Release 1.3 Provisioning Guide*

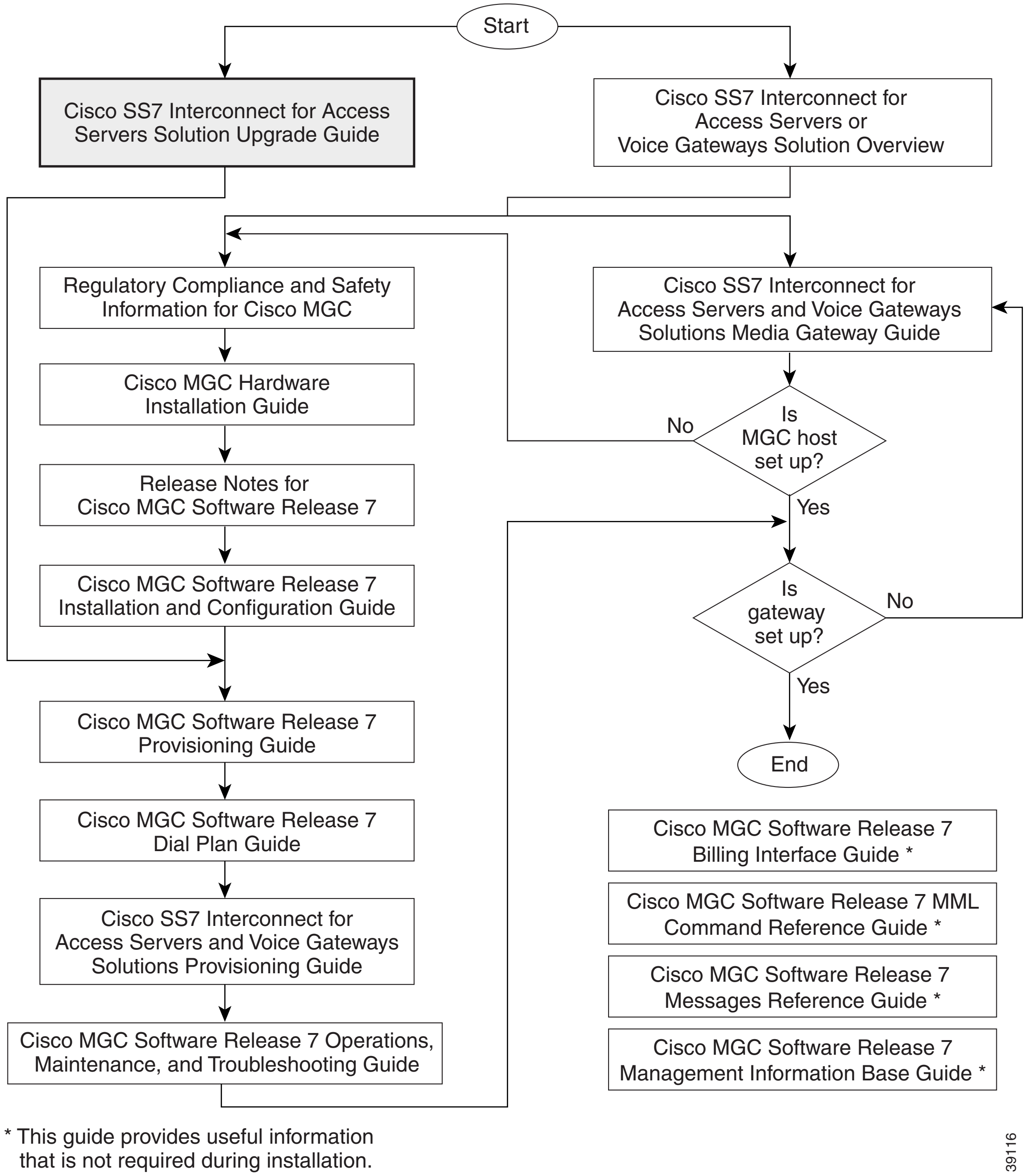
Related Documentation

Consult the following documents for information about the Cisco SC2200:

- *Regulatory Compliance and Safety Information for Cisco Media Gateway Controller Hardware*
- *Cisco Media Gateway Controller Hardware Installation Guide*
- *Release Notes for Cisco Media Gateway Controller Software Release 7*
- *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 Dial Plan Guide*
- *Cisco Media Gateway Controller Software Release 7 Operations, Maintenance, and Troubleshooting Guide*
- *Cisco Media Gateway Controller Software Release 7 MML Command Reference Guide*
- *Cisco Media Gateway Controller Software Release 7 Messages Reference Guide*
- *Cisco Media Gateway Controller Software Release 7 Billing Interface Guide*
- *Cisco Media Gateway Controller Software Release 7 Management Information Base Guide*

Figure 1 shows the sequence in which the various manuals documenting the Cisco SS7 Interconnect for Access Servers and Voice Gateways Solutions should be read.

Figure 1 Documentation Map


Start
Cisco SS7 Interconnect for Access Servers Solution Upgrade Guide
Cisco SS7 Interconnect for Access Servers or Voice Gateways Solution Overview
Regulatory Compliance and Safety Information for Cisco MGC
Cisco SS7 Interconnect for Access Servers and Voice Gateways Solutions Media Gateway Guide
Cisco MGC Hardware Installation Guide
No
Is MGC host set up?
Release Notes for Cisco MGC Software Release 7
Yes
Cisco MGC Software Release 7 Installation and Configuration Guide
Is gateway set up?
No
Yes
Cisco MGC Software Release 7 Provisioning Guide
End
Cisco MGC Software Release 7 Dial Plan Guide
Cisco MGC Software Release 7 Billing Interface Guide *
Cisco MGC Software Release 7 MML Command Reference Guide *
Cisco SS7 Interconnect for Access Servers and Voice Gateways Solutions Provisioning Guide
Cisco MGC Software Release 7 Messages Reference Guide *
Cisco MGC Software Release 7 Operations, Maintenance, and Troubleshooting Guide
Cisco MGC Software Release 7 Management Information Base Guide *
* This guide provides useful information that is not required during installation.
39116

Obtaining Documentation

These sections explain how to obtain documentation from Cisco Systems.

World Wide Web

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

http://www.cisco.com

Translated documentation is available at this URL:

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

Documentation CD-ROM

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

Ordering Documentation

You can order Cisco documentation in these ways:

- Registered Cisco.com users (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 Systems Corporate Headquarters (California, U.S.A.) at 408 526-7208 or, elsewhere in North America, by calling 800 553-NETS (6387).

Documentation Feedback

You can submit comments electronically on Cisco.com. In the Cisco Documentation home page, click the **Fax** or **Email** option in the “Leave Feedback” section at the bottom of the page.

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

You can submit your comments by mail by using the response card behind the front cover of your document or by writing to the following address:

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

We appreciate your comments.

Obtaining Technical Assistance

Cisco provides Cisco.com as a starting point for all technical assistance. Customers and partners can obtain online documentation, troubleshooting tips, and sample configurations from online tools by using the Cisco Technical Assistance Center (TAC) Web Site. Cisco.com registered users have complete access to the technical support resources on the Cisco TAC Web Site.

Cisco.com

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

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

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

If you want to obtain customized information and service, you can self-register on Cisco.com. To access Cisco.com, go to this URL:

http://www.cisco.com

Technical Assistance Center

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

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

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

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

Cisco TAC Web Site

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

http://www.cisco.com/tac

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

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

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

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

If you have Internet access, we recommend that you open P3 and P4 cases through the Cisco TAC Web Site.

Cisco TAC Escalation Center

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

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

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

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

CHAPTER 1

Solution-Level Upgrade Procedures

Solutions Overview

The Cisco SS7 Interconnect for Access Servers Solution is a distributed system used for interconnecting Cisco network access servers (NASs) to a circuit-switched time division multiplexing (TDM) network using Signaling System 7 (SS7) protocols for signaling. The interconnections are achieved using a protocol conversion platform called the Cisco Signaling Controller (also referred to as the Cisco SC2200 product) combined with the Cisco Signaling Link Terminal (Cisco SLT). The Cisco SC2200 comprises the 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.

The Cisco SS7 Dial Access Solution Release 2.0 provided the Cisco signaling controller using T1/E1 or V.35 signaling cards to terminate SS7 signaling from the public switched telephone network (PSTN) and control bearer traffic on the NASs. The Cisco SS7 Interconnect for Access Servers Solution uses the Cisco SLTs instead of cards in the SC host to terminate the first and second MTP layers of SS7 signaling. Bearer traffic remains on the NASs. The use of Cisco SLTs provides redundancy and ensures no disruption of service; this feature was not available with the signaling cards in the SC host in the Cisco SS7 Dial Access Solution Release 2.0.

Use of T1/E1 or V.35 signaling cards is supported for existing installations, but Cisco strongly recommends upgrading to Cisco SLTs to terminate signaling.

Note The Cisco SLT can be located remotely from the Cisco SC host using a dedicated link. Refer to the Cisco SLT documentation for details.

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 SC2200 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.

The Cisco SS7 Interconnect for Voice Gateways Solution also uses the Cisco SLTs to terminate the first and second MTP layers of SS7 signaling. Bearer traffic remains on the voice gateways.

The upgrade process for the Cisco SS7 Interconnect for Access Servers and Voice Gateways Solutions is described in the following sections:

- Before Starting the Upgrade, page 1-2
- Upgrade Procedures, page 1-19

Before Starting the Upgrade

The information you need to be aware of before upgrading is found in the following sections:

- General Tips, page 1-2
- Gathering Required Software and Hardware, page 1-3
- Gathering Provisioning Data, page 1-4
- Minimum SC Hardware Requirements, page 1-17
- SC Software Requirements, page 1-18
- Solution-Specific Requirements, page 1-18

General Tips

Before you upgrade the SC host software, check the following:

- Begin the upgrade process during a maintenance window or low traffic period to minimize call attempt losses, and plan for system downtime accordingly. In a simplex configuration, the host stops processing calls at the beginning of the upgrade. In a continuous service configuration, the standby SC host is upgraded. Calls would only be lost if a failure occurred on the active SC host during the upgrade process.

Caution If you upgrading from the Cisco SS7 DAS Release 2.0 to the Cisco SS7 Interconnect for Access Servers Solution, all calls will be lost during the upgrade, because you cannot switchover from SC Software Release 4 to SC Software Release 7. You can, however, minimize downtime by preparing the new components of your solution, such as setting up hardware and installing software, before you begin. You should also coordinate with your SS7 link service provider to let them know that your links will go out of service. Your provider should have onsite support staff available to assist you should there be problems reestablishing the links.

- Have your company's internal support information and Cisco Systems support contact information available to help you with the installation or upgrade if needed. (See the "Obtaining Technical Assistance" section on page xviii for Cisco support contact information.) Depending on your level of UNIX expertise, you might need to have your UNIX system administrator available for assistance during the upgrade.
- Review the software terms and conditions.
- Review the software and tool requirements and procedural overview.
- Review the hardware and software requirements found in the *Release Notes for the Cisco SS7 Interconnect for Access Servers Solution* or *Release Notes for the Cisco SS7 Interconnect for Voice Gateways Solution.*
- Ensure that all systems are working properly and that there are no alarms.

Note Monitor system output frequently for error messages during the upgrade process. Correct any error messages before continuing with the upgrade.

Gathering Required Software and Hardware

Gather all required software and hardware. Refer to “Minimum SC Hardware Requirements” section on page 1-17 and “SC Software Requirements” section on page 1-18. At a minimum, you must obtain the following CD-ROM disks:

- Sun Solaris^{TM} Operating Environment Installation CD, September 1999, p/n: 704-6914-10
- Sun Solaris^{TM} 2.6 Software, p/n: 704-6220-10
- Sun Solaris^{TM} 2.5.1 Software, to be used if you need to back out of the Sun Solaris^{TM} 2.6 upgrade and reinstall Sun Solaris^{TM}.
- Cisco Telephony Controller Software Release 7.3(x) CD or Cisco Media Gateway Controller Release 7.4(x) CD
- Cisco MGC Installation CD—Includes software for Sun Solaris^{TM} Y2K patches, Volume Manager software, and the log and spool software.

Note Obtain the Volume Manager License key from Sun Microsystems using the software license key request form that is ordered with the target machine. Follow the instructions on the form to obtain a Volume Manager License Key.

- Sun Netra t 112x CD, if installing alarm card software.

The target machine must have a terminal connected by using a serial cable inserted into the console port.

Gathering Required Information

You need the following information for the upgrade:

- SC host server name and IP address
- Root password
- Subnet netmask

Reviewing Your Components.dat and Properties.dat Files for Potential Problems

If you are upgrading a Cisco SS7 DAS Release 2.0 system, you must review your components.dat and properties.dat files to determine whether long file names or special characters such as periods, symbols, or spaces are used. The migration between Software Release 4 and Software Release 7.3(x) requires that MML names of components be 10 alphanumeric characters or less, begin with a character, and cannot contain special characters. MML names can contain dashes. (In Software Release 7.4(x), MML names must be 20 characters or less and meet the same standards.)

To review these files:

Step 1 Change to the /opt/TransPath/etc directory.

Step 2 View the components.dat and properties.dat files. For example, the following components.dat file has long file names that will cause the migration to fail:

```
# cd /opt/TransPath/etc
# more components.dat
00010001  00000000  "LPC-01"                "TransPath: SC07  SC-Pod7-TP"
00020001  00010001  "CFGG-01"               "Config Mgr Subsystem"
00020002  00010001  "ALGG-01"               "Alarm Mgr Subsystem"
00020003  00010001  "MSGG-01"               "Measurement Mgr Subsystem"
00020004  00010001  "ENGG-01"               "Engine Subsystem"
00020005  00010001  "IOSG-01"               "IO Subsystem"
00020006  00010001  "LOGM-01"               "Log Manager Subsystem"
00020007  00010001  "XEG-01"                "Execution Environment Daemons"
00020008  00010001  "PFMG-01"               "Platform Monitoring"
00030001  00020007  "CFM-01"                "Config Manager"
00030002  00020007  "ALM-01"                "Alarm Manager"
00030003  00020007  "MM-01"                 "Measurement Manager"
00030004  00020007  "DMPR-01"               "Data Dumper"
00030005  00020008  "DSKM-01"               "Disk Space Monitor"
00030006  00020004  "ENG-01"                "Engine"
00030007  00020005  "IOCM-01"               "IOS Channel Manager"
00030008  00020005  "IOCC-ASP"              "IOS Channel Controller - ASP"
0003000A  00020007  "SNMP-AGT"              "SNMP Agent Subsystem"
0003000B  00020005  "IOCC-02"               "IOS Channel Controller - ANSI-SS7"
0003000C  00020005  "IOCC-01"               "IOS Channel Controller - ISDNPRI-IP"
00040001  00010001  "CPU-01"                "CPU 1"
00040003  00010001  "DISK-01"               "Hard Disk #1"
00040004  00010001  "DISK-02"               "Hard Disk #2"
00050001  00010001  "SS7-Link-STP-A"        "SS7-Link-STP-A: STP-A-SS7-linkset"
00050002  00010001  "ss7-Link-STP-B"        "ss7-Link-STP-B: tester1"
00050003  00010001  "EN-1"                  "EN-1: Ethernet 1"
00050004  00010001  "EN-2"                  "EN-2: Ethernet 2"
00060001  00050001  "L-ss7-Link-STP-B-0"    "L-ss7-Link-STP-B-0: 5-E"
```

In this example, the SS7-Link-STP-A, SS7-Link-STP-B, and L-SS7-Link-STP-B-0 components are invalid.

Step 3 Use a text editor such as vi to edit the file and rename the invalid components.

Caution If you do not edit MML names to conform to the new restrictions, your installation migration will fail. You will have to edit the names and reinstall package CSCOgc001.

Gathering Provisioning Data

Gather provisioning information in order to quickly provision your system after upgrading. You should read the *Cisco Media Gateway Controller Software Release 7 Provisioning Guide* and use the worksheets below to list the components in your network that you need to provision. Also refer to the *Cisco SS7 Interconnect for Access Servers and Voice Gateways Solutions Provisioning Guide* or the *Cisco SS7 Interconnect for Voice Gateways Solution Release 1.3 Provisioning Guide* for further instructions. Advance preparation will greatly lessen the time required to complete the provisioning during the upgrade.

To provision, you can use the command line interface, MML, or a Cisco-provided GUI provisioning tool. The following GUI provisioning tools are available for your SC software:

- Telephony Controller Manager (TCM)—Available only with software release 7.3(x)
- Cisco Media Gateway Controller Manager (CMM)—Available with software release 7.4(x) and later versions of software release 7.3
- Voice Services Provisioning Tool (VSPT)—Available with later versions of software release 7.4(x)

Timesaver To save time, you can use an MML batch file to provision your system. This requires that you enter all MML commands to provision your system into an ASCII text file and import the file. See the *Cisco SS7 Interconnect for Access Servers Solution Provisioning Guide* or *Cisco SS7 Interconnect for Voice Gateways Provisioning Guide* for more information and a sample batch file.

Completing the following worksheets will help you in provisioning your system.

Point Codes

To define SS7 network addresses, you must configure the following component types:

- Provisioning Tool Component Name: PointCode
- MML Component Name: PTCODE
- GUI Provisioning Tool Component Name: APC
- MML Component Name: APC

Table 1-1 Point Code Parameter Descriptions

MML Parameter Name	Provisioning Tool Parameter Name	Description
NAME	MML Name	Unique name for this point code. Enter as many as 10 alphanumeric characters (or 20 alphanumeric characters for Release 7.4) and enclose in straight quotes. Dashes (-) can be used.
NETADDR	Network Address	SS7 network address in dotted notation.
NETIND	Network Indicator	The network indicator assigned by the network administrator.
DESC	Description	Text description of this point code. Enter as many as 128 characters and enclose in straight quotes.

Table 1-2 Point Code Configuration Parameters

NAME	NETADDR	NETIND	DESC

Table 1-2 Point Code Configuration Parameters (continued)

NAME	NETADDR	NETIND	DESC

Table 1-3 Adjacent Point Code Configuration Parameters

NAME	NETADDR	NETIND	DESC

Linksets

To define linksets, you must configure the following component types:

- GUI Provisioning Tool Component Name: LinkSet
- MML Component Name: LNKSET

Note When configuring linksets for STP connections, you will usually configure two linksets for each pair of STPs.

Table 1-4 Linkset Configuration Parameter Descriptions

MML Parameter Name	Provisioning Tool Parameter Name	Description
NAME	MML Name	Unique name for this linkset. Enter as many as 10 characters (or 20 alphanumeric characters for Release 7.4) and enclose in straight quotes. Dashes (-) can be used.
APC	Adjacent Point Code/Point Code	Adjacent point code or destination point code. For linksets that connect directly to an SSP, enter the MML name of a previously defined destination point code. For linksets that connect to a Cisco SLT, enter the MML name of a previously defined adjacent point code.

Table 1-4 Linkset Configuration Parameter Descriptions (continued)

MML Parameter Name	Provisioning Tool Parameter Name	Description
TYPE	Transport Type	Enter **TDM** for linksets that connect directly to an SSP, or enter **IP** for linksets that connect to Cisco SLTs. The default is TDM.
PROTO	Protocol Family	Enter one of the following: SS7-ANSI SS7-ITU SS7-China SS7-UK
DESC	Description	Text description of this linkset. Enter as many as 128 characters and enclose in straight quotes.

Table 1-5 Linkset Configuration Parameters

Name	APC or DPC	Type	Proto	Desc

SS7 Subsystem

To define an SS7 subsystem, you must configure the following component types:

- GUI Provisioning Tool Component Name: SS7SubSys
- MML Component Name: SS7SUBSYS

For mated STPs, the subsystem defined for each STP defines the other STP as the mate using the MATEDAPC parameter.

Table 1-6 SS7 Subsystem Configuration Parameter Descriptions

MML Parameter Name	Provisioning Tool Parameter Name	Description
NAME	MML Name	Unique name for this subsystem. Enter as many as 10 alphanumeric characters (or 20 alphanumeric characters for Release 7.4) and enclose in straight quotes. Dashes (-) can be used.
SVC	Adjacent Point Code	Adjacent point code for an STP. The MML name or index of the APC if TRANSPROTO is SCCP. Or the MML name or index of TCAPOverIP service for IN trigger services if TRANSPROTO is TCPIP. Enter the MML name of a previously defined APC.
MATEDAPC	Mated Adjacent Point Code	Adjacent point code for an STP mate. Enter the MML name of previously defined APC. Only used when mating STPs, not when creating AIN subsystems.

Table 1-6 SS7 Subsystem Configuration Parameter Descriptions (continued)

MML Parameter Name	Provisioning Tool Parameter Name	Description
PRI	Priority	Priority. Enter an integer that is greater than 0 and less than 4. One (1) is the highest priority level. When two subsystems share the same priority level, traffic is shared by both subsystems. Not used when mating STPs. Default = 1.
PROTO	Protocol Family	Protocol family. When mating STPs, only the SS7 variant is allowed. • SS7-ANSI - when creating an AIN subsystem. • SS7-ITU - when creating an AIN subsystem. • SS7-China - when mating an STP pair. • SS7-UK - when mating an STP pair. If the SVC is an APC, SCCP should not be used (SCCP is not used when mating STP pairs. If the SVC is a TCAPoverIP service, then TCPIP should be used
SSN	Sub System Number	Subsystem number. Enter an integer from 0 to 255. When mating STPs, SSN = 0. When using IN services, SSN can be set to a value greater than 0. Default = 0.
STPSCPIND	STP-SCP Index	STP/SCP index. Enter an integer greater than 0. When mating STPs = 0. Default = 0. Not used when mating STPs.
TRANSPROTO	Transport Protocol	Transport protocol. Enter the transport protocol of this subsystem. When mating STPs = SCCP. Values: SCCP or TCPIP. Not used when mating STPs.

Table 1-7 SS7 Subsystem Configuration Parameters

Name	APC	Mated APC	Pri	Proto	SSN	Desc

SS7 Route

To define an SS7 route, you must configure the following component types:

- GUI Provisioning Tool Component Name: SS7Route
- MML Component Name: SS7ROUTE

Table 1-8 SS7 Route Configuration Parameter Descriptions

MML Parameter Name	Provisioning Tool Parameter Name	Description
NAME	MML Name	Unique name for this route. Enter as many as 10 alphanumeric characters (or 20 alphanumeric characters for Release 7.4) and enclose in straight quotes. Dashes (-) can be used.
OPC	Originating Point Code	Origination point code. Enter the MML name of a previously defined origination point code for this SC node.
DPC	Destination Point Code	Destination point code. Enter the MML name of a previously defined destination point code for a remote switch.
LNKSET	Link Set	Linkset that leads to the destination device. Enter the MML name of a previously defined linkset.
PRI	Priority	SS7 route priority. Enter an integer that is greater than 0. One (1) is the highest priority level. When two SS7 routes share the same priority level, traffic is shared by both routes. Default = 1.
DESC	Description	Text description of this route. Enter as many as 128 characters and enclose in straight quotes.

Table 1-9 SS7 Route Configuration Parameters

NAME	OPC	DPC	LINKSET	PRI	DESC

SS7 Signaling Service

To define an SS7 signaling service, you must configure the following component types:

- GUI Provisioning Tool Component Name: SigSS7
- MML Component Name: SS7PATH

Table 1-10 SS7 Signaling Service Configuration Parameter Descriptions

MML Parameter Name	Provisioning Tool Parameter Name	Value	Description
NAME	MML Name		Unique name for this signaling service. Enter as many as 10 alphanumeric characters (or 20 alphanumeric characters for Release 7.4) and enclose in straight quotes. Dashes (-) can be used.
DESC	Description		Text description of this signaling service. Enter as many as 128 characters and enclose in straight quotes.

Table 1-10 SS7 Signaling Service Configuration Parameter Descriptions (continued)

MML Parameter Name	Provisioning Tool Parameter Name	Value	Description
DPC	Point Code		Destination point code. Enter the MML name of a previously defined destination point code.
MDO	MDO File Name		Message definition object file name. Choose the MDO filename that was used in your previous configuration.
SIDE	Side	network	Q.931 call model side. Enter **user** for user side or **network** for network side. Default = network.
CUSTGRPID	Customer Group ID	0000	Customer Group ID. Virtual network identification characters (formerly called the Closed User Group). Values accepted for this field depend on the use of the D channel. Used to retrieve information about this signaling service and which dial plan to use. Enter the four-digit ID. Default = 0000.
CUSTGRP TBL	Customer Group Table	NA	Reserved for future use.

Table 1-11 SS7 Signaling Service Configuration Parameters

NAME	DPC	MDO	Side	CUSTGRPID

Ethernet Cards

To provision network cards, you must configure the following component types:

- GUI Provisioning Tool Component Name: Adapter
- MML Component Name: CARD

Table 1-12 describes configuration parameters you can use to configure cards, and Table 1-13 serves as a form on which you can plan card configurations.

Table 1-12 Card Configuration Parameter Descriptions for Cisco SLT Communications

MML Parameter Name	Provisioning Tool Parameter Name	Default Value	Description
NAME	MML Name	None	Unique name for this component. Enter as many as 10 alphanumeric characters (or 20 alphanumeric characters for Release 7.4) and enclose in straight quotes. Dashes (-) can be used.
SLOT	Slot	None	Location of card or adapter within the host machine. Acceptable values depend on the host machine. The first slot is usually 0. Enter a value from 0 through 15.
TYPE	Type	None	The interface card type. This should be EN for Ethernet cards. The ITK and V35 types are no longer supported for use with the Cisco SC software
DESC	Description	None	Text description of this component point code. Enter as many as 128 characters and enclose in straight quotes.

Table 1-13 Card Configuration Parameters

NAME	SLOT	TYPE	DESC

Ethernet Interfaces

To provision Ethernet interfaces, you must configure the following component types:

- GUI Provisioning Tool Component Name: EnetIF
- MML Component Name: ENETIF

Table 1-14 describes the configuration parameters that define an Ethernet interface. Table 1-15 serves as a form for you to plan the Ethernet interfaces.

Table 1-14 Ethernet Interface Configuration Parameter Descriptions

MML Parameter Name	Provisioning Tool Parameter Name	Description
NAME	MML Name	Unique name for this interface. Enter as many as 10 alphanumeric characters (or 20 alphanumeric characters for Release 7.4) and enclose in straight quotes. Dashes (-) can be used.
CARD	Ethernet Adapter	Identifies the card that supports this interface. Set this to the MML name of a card that has already been defined.
DESC	Description	Text description of this interface. Enter as many as 128 characters and enclose in straight quotes.

Table 1-15 Ethernet Interface Configuration Parameters

NAME	CARD	DESC

C7 IP Links

To provision the Cisco SLT links, you must configure the following component types:

- GUI Provisioning Tool Component Name: C7IPLink
- MML Component Name: C7IPLNK

Table 1-16 lists and describes the C7 IP link configuration parameters that define each link. Table 1-17 serves as a form for planning a single C7 IP link.

Table 1-16 C7 IP Link Configuration Parameter Descriptions

MML Parameter Name	Provisioning Tool Parameter Name	Default Value	Description
NAME	MML Name	None	Unique name for this link. Enter as many as 10 alphanumeric characters (or 20 alphanumeric characters for Release 7.4) and enclose in straight quotes. Dashes (-) can be used.
DESC	Description	None	Text description of this link. Enter as many as 128 characters and enclose in straight quotes.
IF	Enet Line Interface	None	Ethernet interface to which this link connects. Enter the MML name of a previously defined Ethernet interface, or enter the SNMP index number for the interface.
IPADDR	IP Address	None	Cisco SC host IP address for interface. Enter the IP address variable defined in the XECfgParm.dat file during the installation of the Cisco SC software. Valid entries are IP_Addr1, IP_Addr2, IP_Addr3, and IP_Addr4.
LNKSET	Link Set	None	Linkset to which this link belongs. Enter the MML name of a previously defined linkset.
PORT	Port	None	Cisco SC host port number to which this link connects. Enter any valid IP port number. Value range: any valid IP port number from 1025 through 32766.
PEERADDR	Peer Address	None	Remote IP address (in dotted notation) of the Cisco SLT interface to which this link connects. (May also be specified as a host name or a DNS name.)
PRI	Priority	1	Priority. Enter an integer greater than 0. Value range: 1 through 16.

Table 1-16 C7 IP Link Configuration Parameter Descriptions (continued)

MML Parameter Name	Provisioning Tool Parameter Name	Default Value	Description
SLC	Link Code	1	SS7 Signaling link code. Value range: 0 through 15.
TIMESLOT	Time Slot	0	Time slot field for the C7 IP link. Identifies the physical WAN interface card (WIC) slot, or the SS7 serial port, of the Cisco SLT. Value range: 0 through 3.

Table 1-17 C7 IP Link Configuration Parameters

MML Parameter Name	Configuration Setting
DESC	
IF	
IPADDR	
LNKSET	
NAME	
PORT	
PEERADDR	
PRI	
SLC	
TIMESLOT	

NAS External Nodes

To provision media gateway external nodes, you must configure the following component types:

- GUI Provisioning Tool Component Name: ExtNode
- MML Component Name: EXTNODE

Table 1-18 describes the external node configuration parameters, and Table 1-19 serves as a form for you to plan a unique name for each media gateway.

Table 1-18 External Node Configuration Parameter Descriptions

MML Parameter Name	Provisioning Tool Parameter Name	Default Value	Description
NAME	MML Name	None	Unique name for an external device. Enter as many as 10 alphanumeric characters (or 20 alphanumeric characters for Release 7.4) and enclose in straight quotes. Dashes (-) can be used.
DESC	Description	None	Text description of an external device. Enter as many as 128 characters and enclose in straight quotes.

Table 1-19 Media Gateway External Node Configuration Parameters

NAME	DESC

NAS Signaling Service

To provision a NAS signaling service, you must configure the following component types:

- GUI Provisioning Tool Component Name: SigNAS
- MML Component Name: NASPATH

Table 1-20 Media Gateway Signaling Service Configuration Parameter Descriptions

MML Parameter Name	Provisioning Tool Parameter Name	Default Value	Description
NAME	MML Name	None	Unique name for this signaling service. Enter as many as 10 alphanumeric characters (or 20 alphanumeric characters for Release 7.4) and enclose in straight quotes. Dashes (-) can be used.
MDO	MDO File Name	None	Enter a valid message definition object (MDO) file protocol name by using the **PROV-RTRV:VARIANTS** MML command.
EXTNODE	External Node	None	Enter the external node name assigned to the media gateway you are configuring.

Table 1-20 Media Gateway Signaling Service Configuration Parameter Descriptions (continued)

MML Parameter Name	Provisioning Tool Parameter Name	Default Value	Description
SIDE	Side	Network	Q.931 call model side. Enter **user** for user side or **network** for network side. Default = network. (Used only for IP FAS transport service.)
CUSTGRPID	Customer Group ID	0000	Customer Group ID. Virtual network identification characters (formerly called the VNET ID). Values accepted for this field depend on the use of the D channel. Enter the four-digit ID. (Used only for IP FAS transport service.)
CUSTGRP TBL	Customer Group Table	NA	Reserved for future use.
ABFLAG	A/B flag	N	A/B flag. Specifies digital private network signaling system (DPNSS) a or b side. Enter **A** for a side, **B** for b side, or **N** for not applicable. (Used only for IP FAS transport service.)
CRLEN	Call Reference Length	2	Call reference length. Enter **0** for DPNSS, **1** for one-byte call reference, or **2** for two-byte call reference. Default = 2. (Used only for IP FAS transport service.)
DESC	Description	None	Text description of this signaling service. Enter as many as 128 characters and enclose in straight quotes.

Table 1-21 Media Gateway Signaling Service Configuration Parameters

MML Parameter Name	Configuration Setting
NAME	
MDO	
EXTNODE	
DESC	

IP Links

To provision a media gateway IP link, you must configure the following component types:

- GUI Provisioning Tool Component Name: IPLink
- MML Component Name: IPLNK

Table 1-22 lists and describes the configuration parameters that define each link. Table 1-23 serves as a form for planning a single IP link.

Table 1-22 IP-Link Configuration Parameter Descriptions

MML Parameter Name	Provisioning Tool Parameter Name	Default Value	Description
NAME	MML Name	None	Unique name for this link. Enter as many as 10 alphanumeric characters (or 20 alphanumeric characters for Release 7.4) and enclose in straight quotes. Dashes (-) can be used.
IF	Enet Line Interface	None	Ethernet interface to which this link connects. Enter the MML name of a previously defined Ethernet interface.
DESC	Description	None	Text description of this link. Enter as many as 128 characters and enclose in straight quotes.
IPADDR	IP Address	None	Cisco SC host IP address for interface. Enter the IP address variable defined in the XECfgParm.dat file during the installation of the Cisco SC software. Valid entries ar: IP_Addr1, IP_Addr2, IP_Addr3, or IP_Addr4.
PEERADDR	Peer Address	None	Remote IP address of link interface on media gateway.
PEERPORT	Peer Port	None	Port number of link interface on remote device. Enter any valid IP port number greater than 1024. For MGCP and SGCP, 2427 is recommended.
PORT	Port	None	Local port number of link interface on the Cisco SC host. Enter any valid IP port number greater than 1024.
PRI	Priority	1	Priority. Enter an integer that is greater than 0.
SIGPORT	Signal Port	0	Physical port on the gateway on the slot.Value range: 0 through 168. (Used only to support IPFAS.)
SIGSLOT	Signal Slot	0	Physical slot on the gateway where the T1/E1 is plugged into. Value range: 0 through 63. (Used only to support IPFAS.)
SVC	IP Signaling Services	None	Signaling service this IP supports. Enter the MML name of a previously defined signal service.
SIGPORTSKIP		0	Signal port skip. The number of SIGPORT values to be skipped before using the next value. (Used only for NFAS signaling type.)

Table 1-23 IP-Link Configuration Parameters

MML Parameter Name	Value
NAME	
IF	
DESC	
IPADDR	
PEERADDR	
PEERPORT	
PORT	

Table 1-23 IP-Link Configuration Parameters (continued)

MML Parameter Name	Value
PRI	
SIGPORT	
SIGSLOT	
SVC	

Minimum SC Hardware Requirements

Your system must meet the minimum requirements shown in the following tables. If your system does not meet these requirements, you must upgrade components. See Chapter 2, "Backing Up Your SC Host Data," and Chapter 5, "Upgrading SC Host Hardware."

Caution The amount and speed of hardware such as processors and memory strongly impacts the call processing power and speed of the Cisco SS7 Interconnect for Access Servers and Voice Gateways Solutions. Before using the minimum hardware configuration, consult with your Cisco representative to determine the hardware that will give you the best results based on your network configuration, proposed traffic, and desired processing power. In particular, B-number analysis or screening, long call hold times, and SCP queries may require additional hardware resources.

Note Always consult the latest version of the *Release Notes for the Cisco SS7 Interconnect for Access Servers Solution* or *Release Notes for the Cisco SS7 Interconnect for Voice Gateways Solution* (available from Cisco.com) to determine whether any new or additional hardware or software is required.

SC Host Minimum Server Requirements

Table 1-24 shows the SC host minimum hardware requirements.

Note The Sun E450 server is no longer supported for use with the Cisco SC software.

Table 1-24 Host Minimum Hardware Requirements

Component	Sun Netra t 100/105	Sun Netra t 1120/1125	Sun Netra t1400/t1405
Processor	one 440 MHz	two 440 MHz	four 440 MHz
Disk drive	two 18-gigabyte	two 18-gigabyte	two 18-gigabyte
CD-ROM/DVD drive	1CD-ROM drive	1DVD drive	1DVD drive
DAT 3-Drive	N/A	1	1
RAM	1 gigabyte	2 gigabyte	4 gigabyte

Interface Options

Table 1-25 shows the signaling and Ethernet interface options.

Note The ITK E1/T1 and the PTI V.35 interface cards are no longer supported for use with the Cisco SC software.

Table 1-25 Interface Options

Interface Options	Sun Netra t 100/105	Sun Netra t 1120/1125	Sun Netra t1400/t1405
Sun Ethernet 1-port card	N/A (comes equipped with two Ethernet ports)	Required	Required
Cisco SLT	Supported	Supported	Supported

Ancillary Hardware

The following pieces of ancillary hardware are no longer supported for use with the Cisco SC software:

- Dataprobe ARU
- Dataprobe A/B Switch
- Asynch Extension

SC Software Requirements

The SC host requires the software listed below for the Cisco SS7 Interconnect for Access Servers and Voice Gateways Solutions. Gather the required software before beginning the upgrade.

- Sun Solaris 2.6
- Veritas Volume Manager 2.6 (for mirrored drives only)
- Cisco Telephony Controller Software Release 7.3(x) or Cisco Media Gateway Controller Software Release 7.4(x)
- Cisco MGC Installation CD

Note A minimum of 2 gigabytes of swap space is required for the Cisco SS7 Interconnect for Access Servers and Voice Gateways Solutions

Solution-Specific Requirements

To determine the latest hardware and software requirements for your solution, see the following online documents:

- *Release Notes for Cisco SS7 Interconnect for Access Servers Release 2.2(B)*
- *Release Notes for Cisco SS7 Interconnect for Voice Gateways Release 1.3*

Upgrade Procedures

This section provides the upgrade procedures for the Cisco SS7 Interconnect for Access Servers and Voice Gateways Solutions, as described in the following sections:

- Upgrading from the Cisco SS7 DAS Release 2.0 to the Cisco SS7 Interconnect for Access Servers Solution Release 2.x, page 1-19
- Upgrading within the Cisco SS7 Interconnect for Access Servers Solution, from Release 2.1 to Release 2.2, page 1-22
- Upgrading within the Cisco SS7 Interconnect for Voice Gateways Solution, from Release 1.0 or 1.1 to Release 1.3, page 1-25

Upgrading from the Cisco SS7 DAS Release 2.0 to the Cisco SS7 Interconnect for Access Servers Solution Release 2.x

Upgrading from the Cisco DAS Release 2.0 to the Cisco SS7 Interconnect for Access Servers Solution is described in the following sections:

- Upgrading a Simplex Configuration, page 1-19
- Upgrading a High-Availability Configuration, page 1-21

Upgrading a Simplex Configuration

To upgrade a simplex configuration, perform the steps in Table 1-26:

Table 1-26 Upgrading a Cisco DAS Release 2.0 System with an SC host in a Simplex Configuration

	Step	Chapter/Section
Step 1	Prepare by gathering the required hardware, software, and information you need to perform the upgrade.	Before Starting the Upgrade, page 1-2
Step 2	Back up your SC host data. **Note** Call processing must be stopped at this time. The SC host will be out of service until the upgrade is completed.	Backing Up Your SC Host Data, page 2-1
Step 3	Upgrade the software on your media gateways. **Note** All calls on the media gateways are dropped during the software upgrade.	Cisco Media Gateway Upgrade Procedures, page 3-1
Step 4	Install and configure Cisco SLTs.	Cisco Signaling Link Terminal Upgrade Procedures, page 4-1
Step 5	If necessary, perform SC host hardware upgrades.	Upgrading SC Host Hardware, page 5-1
Step 6	If necessary, upgrade the operating system and associated software, including: • Sun Solaris 2.6 • Alarm card software • Ethernet interfaces • Second disk drives (for mirrored disks)	Installing the Operating System on the SC Hosts, page 6-1

Table 1-26 Upgrading a Cisco DAS Release 2.0 System with an SC host in a Simplex Configuration (continued)

	Step	Chapter/Section
Step 7	Uninstall the old SC software.	Removing a Previous Version of the Cisco Telephony Controller Software (Release 4 and Release 7.3(x)), page 7-3 or Removing a Previous Version of the Cisco MGC Software (Release 7.4(x)), page 7-4
Step 8	Install the new SC software.	Installing SC Software Release 7.3(x), page 7-5 or Installing SC Software Release 7.4(x), page 7-7
Step 9	Install patches to the new SC software version	Installing Patches for the SC Software, page 7-10
Step 10	Restore your backed up SC software data.	Installing a GUI Provisioning Tool on a Separate Server, page 7-10
Step 11	If necessary, install your GUI provisioning tool on a separate server	Installing a GUI Provisioning Tool on a Separate Server, page 7-10
Step 12	Configure SNMP resources.	Configuring SNMP Support Resources, page 7-13
Step 13	Configure the execution environment parameters.	Configuring the Execution Environment, page 7-19
Step 14	Configure SCP queries.	Configuring SCP Queries, page 7-38
Step 15	Terminate signaling links to Cisco SLTs.	Terminating Signaling Links, page 7-56
Step 16	Start the software on the newly upgraded SC host.	Restarting the SC Software, page 7-56
Step 17	Verify that the newly installed software is working properly.	Verifying SC Software is Running Properly, page 7-59
Step 18	Provision your Cisco SC2200, including Cisco SLTs.	Provisioning the Configuration, page 7-68

Upgrading a High-Availability Configuration

To upgrade a high-availability configuration, perform the steps in Table 1-26:

Table 1-27 Upgrading a Cisco DAS Release 2.0 System with SC hosts in a High Availability Configuration

	Step	Chapter/Section
Step 1	Prepare by gathering the required hardware, software, and information you need to perform the upgrade.	Before Starting the Upgrade, page 1-2
Step 2	Back up your SC host data. **Note** The standby SC host is upgraded, leaving the active SC host to process calls. Unless the active SC host goes down, call processing will not be affected.	Backing Up Your SC Host Data, page 2-1
Step 3	Upgrade the software on your media gateways. **Note** All calls on the media gateways are dropped during the software upgrade.	Cisco Media Gateway Upgrade Procedures, page 3-1
Step 4	Install and configure the Cisco SLTs. **Note** Do not connect the signaling links to the Cisco SLT during this step, or call processing will stop.	Cisco Signaling Link Terminal Upgrade Procedures, page 4-1
Step 5	If necessary, perform SC host hardware upgrades.	Upgrading SC Host Hardware, page 5-1
Step 6	Upgrade the operating system and associated software on the standby SC host, including: • Sun Solaris 2.6 • Alarm card software • Ethernet interfaces • Second disk drives (for mirrored disks)	Installing the Operating System on the SC Hosts, page 6-1
Step 7	Uninstall the old SC software on the standby SC host.	Removing a Previous Version of the Cisco Telephony Controller Software (Release 4 and Release 7.3(x)), page 7-3 or Removing a Previous Version of the Cisco MGC Software (Release 7.4(x)), page 7-4
Step 8	Install the new SC software on the standby SC host.	Installing SC Software Release 7.3(x), page 7-5 or Installing SC Software Release 7.4(x), page 7-7
Step 9	Install patches to the new SC software version	Installing Patches for the SC Software, page 7-10
Step 10	Restore your backed up SC host data files on the standby SC host.	Installing a GUI Provisioning Tool on a Separate Server, page 7-10
Step 11	If necessary, install your GUI provisioning tool on a separate server	Installing a GUI Provisioning Tool on a Separate Server, page 7-10
Step 12	Configure SNMP resources on the standby SC host.	Configuring SNMP Support Resources, page 7-13

Table 1-27 Upgrading a Cisco DAS Release 2.0 System with SC hosts in a High Availability Configuration (continued)

	Step	Chapter/Section
Step 13	Configure the execution environment parameters on the standby SC host. **Note** When you upgrade the first SC host, ensure that the value of *.desiredPlatformState is **Master** and pom.dataSync is **false**. When you upgrade the second SC host, ensure that the value of *.desiredPlatformState is **Slave** and pom.dataSync is **true**.	Configuring the Execution Environment, page 7-19
Step 14	Configure SCP queries on the standby SC host.	Configuring SCP Queries, page 7-38
Step 15	Terminate signaling links to the Cisco SLTs.	Terminating Signaling Links, page 7-56
Step 16	Start the software on the newly upgraded SC host.	Restarting the SC Software, page 7-56
Step 17	Verify that the newly installed software is working properly.	Verifying SC Software is Running Properly, page 7-59
Step 18	Upgrade and verify the other SC host.	Repeat steps 7 through 17 on the other SC host.
Step 19	Reset the value of pom.dataSync to **true** in the first SC host.	Resetting the Configuration, page 7-68
Step 20	Provision your Cisco SC2200, including Cisco SLTs.	Provisioning the Configuration, page 7-68

Upgrading within the Cisco SS7 Interconnect for Access Servers Solution, from Release 2.1 to Release 2.2

Upgrading within the Cisco SS7 Interconnect for Access Servers Solution, from Release 2.1 to Release 2.2 is described in the following sections:

- Upgrading a Simplex Configuration, page 1-22
- Upgrading a Continuous Service Configuration, page 1-24

Upgrading a Simplex Configuration

To upgrade a simplex configuration, perform the steps in Table 1-28:

Table 1-28 Upgrading a Cisco SS7 Interconnect for Access Servers Release 2.1 System with an SC host in a Simplex Configuration

	Step	Chapter/Section
Step 1	Prepare by gathering the required hardware, software, and information you need to perform the upgrade.	Before Starting the Upgrade, page 1-2
Step 2	Back up your SC host data. **Note** Call processing must be stopped at this time. The SC host will be out of service until the upgrade is completed.	Backing Up Your SC Host Data, page 2-1

Table 1-28 Upgrading a Cisco SS7 Interconnect for Access Servers Release 2.1 System with an SC host in a Simplex Configuration (continued)

	Step	Chapter/Section
Step 3	If you are using the Cisco Media Gateway Controller Node Manager (CMNM) software to manage the Cisco SC2200, ensure that you have the latest CMNM patches installed.	Proceed to the CMNM patch web page at the following URL: http://www.cisco.com/cgi-bin/tablebuild.pl/mgc-nm The installation instructions for each patch are found in the associated README files.
Step 4	Upgrade the software on your media gateways. **Note** All calls on the media gateways are dropped during the software upgrade.	Cisco Media Gateway Upgrade Procedures, page 3-1
Step 5	Upgrade the software on the Cisco SLTs.	Cisco Signaling Link Terminal Upgrade Procedures, page 4-1
Step 6	Identify the name of the active configuration.	Identifying the Active Configuration, page 7-2
Step 7	Uninstall the old SC software.	Removing a Previous Version of the Cisco Telephony Controller Software (Release 4 and Release 7.3(x)), page 7-3 or Removing a Previous Version of the Cisco MGC Software (Release 7.4(x)), page 7-4
Step 8	Install the new SC software.	Installing SC Software Release 7.4(x), page 7-7
Step 9	Install patches to the new SC software version	Installing Patches for the SC Software, page 7-10
Step 10	If necessary, install your GUI provisioning tool on a separate server	Installing a GUI Provisioning Tool on a Separate Server, page 7-10
Step 11	Configure SNMP resources.	Configuring SNMP Support Resources, page 7-13
Step 12	Configure the execution environment parameters.	Configuring the Execution Environment, page 7-19
Step 13	Configure SCP queries.	Configuring SCP Queries, page 7-38
Step 14	If you are upgrading from ITK/PTI cards to Cisco SLTs, terminate signaling links to the Cisco SLTs.	Terminating Signaling Links, page 7-56
Step 15	Start the software on the newly upgraded SC host.	Restarting the SC Software, page 7-56
Step 16	Verify that the newly installed software is working properly.	Verifying SC Software is Running Properly, page 7-59
Step 17	If necessary, provision your Cisco SC2200, including Cisco SLTs.	Provisioning the Configuration, page 7-68

Upgrading a Continuous Service Configuration

To upgrade a continuous service configuration, perform the steps in Table 1-29:

Table 1-29 Upgrading a Cisco SS7 Interconnect for Access Servers Solution Release 2.1 System with SC hosts in a Continuous Service Configuration

	Step	Chapter/Section
Step 1	Prepare by gathering the required hardware, software, and information you need to perform the upgrade.	Before Starting the Upgrade, page 1-2
Step 2	Back up your SC host data. **Note** The standby SC host is upgraded, leaving the active SC host to process calls. Unless the active SC host goes down, call processing is not affected.	Backing Up Your SC Host Data, page 2-1
Step 3	If you are using the Cisco Media Gateway Controller Node Manager (CMNM) software to manage the Cisco SC2200, ensure that you have the latest CMNM patches installed.	Proceed to the CMNM patch web page at the following URL: http://www.cisco.com/cgi-bin/tablebuild.pl/mgc-nm The installation instructions for each patch are found in the associated README files.
Step 4	Upgrade the software on your media gateways. **Note** All calls on the media gateways are dropped during the software upgrade.	Cisco Media Gateway Upgrade Procedures, page 3-1
Step 5	Upgrade the software on the Cisco SLTs.	Cisco Signaling Link Terminal Upgrade Procedures, page 4-1
Step 6	Identify the name of the active configuration.	Identifying the Active Configuration, page 7-2
Step 7	Uninstall the old SC software on the standby SC host.	Removing a Previous Version of the Cisco Telephony Controller Software (Release 4 and Release 7.3(x)), page 7-3 or Removing a Previous Version of the Cisco MGC Software (Release 7.4(x)), page 7-4
Step 8	Install the new SC software on the standby SC host.	Installing SC Software Release 7.4(x), page 7-7
Step 9	Install patches to the new SC software version	Installing Patches for the SC Software, page 7-10
Step 10	If necessary, install your GUI provisioning tool on a separate server	Installing a GUI Provisioning Tool on a Separate Server, page 7-10
Step 11	Check the value of pom.dataSync. When you upgrade the first SC host, ensure that the value of pom.dataSync is **false**. When you upgrade the second SC host, ensure that the value of pom.dataSync is **true**.	Opening the XECfgParm.dat File, page 7-20, Initializing the Provisioning Object Manager (POM), page 7-37, and Saving the XECfgParm.dat File, page 7-37
Step 12	If you are upgrading from ITK/PTI cards to Cisco SLTs, terminate signaling links to the Cisco SLTs.	Terminating Signaling Links, page 7-56
Step 13	Start the software on the newly upgraded SC host.	Restarting the SC Software, page 7-56
Step 14	Verify that the newly installed software is working properly.	Verifying SC Software is Running Properly, page 7-59
Step 15	Upgrade and verify the other SC host.	Perform steps 6 through 14 on the other SC host.

Table 1-29 Upgrading a Cisco SS7 Interconnect for Access Servers Solution Release 2.1 System with SC hosts in a Continuous Service Configuration (continued)

	Step	Chapter/Section
Step 16	Reset the value of pom.dataSync to **true** in the first SC host.	Resetting the Configuration, page 7-68
Step 17	If necessary, provision your Cisco SC2200, including Cisco SLTs.	Provisioning the Configuration, page 7-68

Upgrading within the Cisco SS7 Interconnect for Voice Gateways Solution, from Release 1.0 or 1.1 to Release 1.3

Upgrading within the Cisco SS7 Interconnect for Voice Gateways Solution, from Release 1.0 or 1.1 to Release 1.3 is described in the following sections:

- Upgrading a Simplex Configuration, page 1-22
- Upgrading a Continuous Service Configuration, page 1-24

Upgrading a Simplex Configuration

To upgrade a simplex configuration, perform the steps in Table 1-30:

Table 1-30 Upgrading a Cisco SS7 Interconnect for Voice Gateways Release 1.0 or 1.1 System with an SC host in a Simplex Configuration

	Step	Chapter/Section
Step 1	Prepare by gathering the required hardware, software, and information you need to perform the upgrade.	Before Starting the Upgrade, page 1-2
Step 2	Back up your SC host data. **Note** Call processing must be stopped at this time. The SC host will be out of service until the upgrade is completed.	Backing Up Your SC Host Data, page 2-1
Step 3	If you are using the Cisco Media Gateway Controller Node Manager (CMNM) software to manage the Cisco SC2200, ensure that you have the latest CMNM patches installed.	Proceed to the CMNM patch web page at the following URL: http://www.cisco.com/cgi-bin/tablebuild.pl/mgc-nm The installation instructions for each patch are found in the associated README files.
Step 4	Upgrade the software on your media gateways. **Note** All calls on the media gateways are dropped during the software upgrade.	Cisco Media Gateway Upgrade Procedures, page 3-1
Step 5	Upgrade the software on the Cisco SLTs.	Cisco Signaling Link Terminal Upgrade Procedures, page 4-1
Step 6	Identify the name of the active configuration.	Identifying the Active Configuration, page 7-2

Table 1-30 Upgrading a Cisco SS7 Interconnect for Voice Gateways Release 1.0 or 1.1 System with an SC host in a Simplex Configuration (continued)

	Step	Chapter/Section
Step 7	Uninstall the old SC software.	Removing a Previous Version of the Cisco Telephony Controller Software (Release 4 and Release 7.3(x)), page 7-3 or Removing a Previous Version of the Cisco MGC Software (Release 7.4(x)), page 7-4
Step 8	Install the new SC software.	Installing SC Software Release 7.4(x), page 7-7
Step 9	Install patches to the new SC software version	Installing Patches for the SC Software, page 7-10
Step 10	If necessary, install your GUI provisioning tool on a separate server	Installing a GUI Provisioning Tool on a Separate Server, page 7-10
Step 11	Start the software on the newly upgraded SC host.	Restarting the SC Software, page 7-56
Step 12	Verify that the newly installed software is working properly.	Verifying SC Software is Running Properly, page 7-59
Step 13	If necessary, provision your Cisco SC2200, including Cisco SLTs.	Provisioning the Configuration, page 7-68

Upgrading a Continuous Service Configuration

To upgrade a continuous service configuration, perform the steps in Table 1-31:

Table 1-31 Upgrading a Cisco SS7 Interconnect for Voice Gateways Solution Release 1.0 or 1.1 System with SC hosts in a Continuous Service Configuration

	Step	Chapter/Section
Step 1	Prepare by gathering the required hardware, software, and information you need to perform the upgrade.	Before Starting the Upgrade, page 1-2
Step 2	Back up your SC host data. **Note** The standby SC host is upgraded, leaving the active SC host to process calls. Unless the active SC host goes down, call processing will not be affected.	Backing Up Your SC Host Data, page 2-1
Step 3	If you are using the Cisco Media Gateway Controller Node Manager (CMNM) software to manage the Cisco SC2200, ensure that you have the latest CMNM patches installed.	Proceed to the CMNM patch web page at the following URL: http://www.cisco.com/cgi-bin/tablebuild.pl/mgc-nm The installation instructions for each patch are found in the associated README files.
Step 4	Upgrade the software on your media gateways. **Note** All calls on the media gateways are dropped during the software upgrade.	Cisco Media Gateway Upgrade Procedures, page 3-1
Step 5	Upgrade the software on the Cisco SLTs.	Cisco Signaling Link Terminal Upgrade Procedures, page 4-1
Step 6	Identify the name of the active configuration.	Identifying the Active Configuration, page 7-2

Table 1-31 Upgrading a Cisco SS7 Interconnect for Voice Gateways Solution Release 1.0 or 1.1 System with SC hosts in a Continuous Service Configuration (continued)

	Step	Chapter/Section
Step 7	Uninstall the old SC software on the standby SC host.	Removing a Previous Version of the Cisco Telephony Controller Software (Release 4 and Release 7.3(x)), page 7-3 or Removing a Previous Version of the Cisco MGC Software (Release 7.4(x)), page 7-4
Step 8	Install the new SC software on the standby SC host.	Installing SC Software Release 7.4(x), page 7-7
Step 9	Install patches to the new SC software version	Installing Patches for the SC Software, page 7-10
Step 10	If necessary, install your GUI provisioning tool on a separate server	Installing a GUI Provisioning Tool on a Separate Server, page 7-10
Step 11	Check the value of pom.dataSync. When you upgrade the first SC host, ensure that the value of pom.dataSync is **false**. When you upgrade the second SC host, ensure that the value of pom.dataSync is **true**.	Opening the XECfgParm.dat File, page 7-20, Initializing the Provisioning Object Manager (POM), page 7-37, and Saving the XECfgParm.dat File, page 7-37
Step 12	Start the software on the newly upgraded SC host.	Restarting the SC Software, page 7-56
Step 13	Verify that the newly installed software is working properly.	Verifying SC Software is Running Properly, page 7-59
Step 14	Upgrade and verify the other SC host.	Perform steps 6 through 13 on the other SC host.
Step 15	Reset the value of pom.dataSync to **true** in the first SC host.	Resetting the Configuration, page 7-68
Step 16	If necessary, provision your Cisco SC2200, including Cisco SLTs.	Provisioning the Configuration, page 7-68

CHAPTER 2

Backing Up Your SC Host Data

Use the instructions in this chapter to back up your current SC software configuration. If you have a simplex SC host configuration, you back up the data on your server after shutting it down. If you have a high-availability or continuous service configuration, bring the standby SC host down and back up the data on the standby SC host first, so the active SC host can still process calls while the standby is being upgraded. This minimizes downtime.

Caution You must back up your data before beginning the upgrade. If you do not back up your data, it will be lost during the upgrade.

Tip Depending on your level of UNIX expertise, you might need to have your UNIX system administrator available for assistance during the upgrade. These instructions might not be sufficient or accurate for large, complex networks.

Caution Do not back up data to an active remote SC host that is processing calls. For example, do not back up your SC host machine to the second host in a high-availability configuration. This can severely impact or shut down call processing.

If you have a high-availability or continuous service configuration, first determine which host is running as active. To determine which host is running as active, log in to each machine and use the **rtrv-ne** MML command. The display shows whether the machine is active or standby.

Select your backup procedure based on your desired storage location, a local tape drive or a remote machine on your network. The procedures are described in the following sections:

- Backing Up Your Data Using a Tape Drive, page 2-1
- Backing Up Your Data to a Remote Machine, page 2-3

Backing Up Your Data Using a Tape Drive

Use these instructions to back up your data to tape. You will restore the data before installing the SC software.

Step 1 Log in to the SC host as root and insert a tape into your tape drive.

Step 2 Stop the SC software by entering the following command:

```
/etc/init.d/transpath stop
```

Note If the standby SC host is running Release 7.4(x), the command to stop the SC software is **/etc/init.d/CiscoMGC stop**.

Note In a simplex configuration, call processing stops now. The SC host is not able to process calls until you restart the software after the upgrade. See the "Verifying SC Software is Running Properly" section on page 7-59. In a high-availability or continuous service configuration, perform these steps on the standby SC host first. Unless the active SC host goes down, call processing does not stop.

Step 3 If your system does *not* have a dial plan configured, proceed to Step 6. If your system has a dial plan configured, backup the contents of the MMDB to a single file, as described in the "Performing a Backup Operation on the Main Memory Database" section on page 2-4.

Step 4 Run the backup script by entering the following command at the UNIX prompt:

```
# ./backup.sh
```

The system returns a response similar to the following:

```
MGC backup utility
-----------------------------
Destination currently set to Local tape (/dev/rmt/0h)
Enter:
    <N> set destination to remote NFS server
    <L> set destination to Local tape (/dev/rmt/0h)
    <F> for Full (everything you have)
    <P> for Partial (changable part of the system)
    <Q> to quit
Select backup mode:
```

Step 5 Enter **F** and press **Enter** to start the full backup. The system returns a message similar to the following:

```
a ./ 0 tape blocks
a ./var/ 0 tape blocks
a ./var/log/ 0 tape blocks
a ./var/log/platform.log 1 tape blocks
a ./var/log/mml.log 1 tape blocks
a ./var/spool/ 0 tape blocks
a ./var/trace/ 0 tape blocks
a ./var/audit_cron.log 1 tape blocks
.
.
.#
```

Step 6 When the backup operation has finished, remove the tape, engage the write-protect tab, and label the tape "Upgrade Backup." Specify the machine name and the time and date.

This completes backing up your SC host data to tape. Return to the your chosen upgrade procedure and continue.

Backing Up Your Data to a Remote Machine

Use these instructions to back up your data to a remote machine using your IP network.

Caution Do not back up your data to another SC host machine. Only use a spare machine that is not processing calls.

Note This procedure backs ups everything in the SC software base directory to an NFS mountable directory on a remote machine. The remote machine must be set up with an NFS mountable directory that is writable by machine being backed up. The NFS set up of the remote machine is beyond the scope of this document; contact your UNIX system administrator for more information.

Step 1 Log in to the SC host as root and stop the SC software by entering the following command:

```
/etc/init.d/transpath stop
```

Note If the standby SC host is running Release 7.4(x), the command to stop the SC software is **/etc/init.d/CiscoMGC stop**.

Note In a simplex configuration, call processing stops now. The SC host is not able to process calls until you restart the software after the upgrade. See the “Verifying SC Software is Running Properly” section on page 7-59. In a high-availability or continuous service configuration, perform these steps on the standby SC host first. Unless the active SC host goes down, call processing does not stop.

Step 2 If your system does *not* have a dial plan configured, proceed to Step 3. If your system has a dial plan configured, backup the contents of the MMDB to a single file, as described in the “Performing a Backup Operation on the Main Memory Database” section on page 2-4.

Step 3 Run the backup script by entering the following command at the UNIX prompt:

```
# ./backup.sh
```

The system returns a response similar to the following:

```
MGC backup utility
-----------------------------
Destination currently set to Local tape (/dev/rmt/0h)
Enter:
    <N> set destination to remote NFS server
    <L> set destination to Local tape (/dev/rmt/0h)
    <F> for Full (everything you have)
    <P> for Partial (changable part of the system)
    <Q> to quit
Select backup mode:
```

Step 4 Select **N** and press **Enter** to define the remote NFS server. The system then prompts you for the name of the remote server.

Step 5 Enter the name of the remote NFS server.

```
Enter server name: remote_hostname
```

Where: *remote_hostname*—Name of your desired remote server.

The system then prompts you for the associated directory name on your remote server.

Step 6 Enter the directory name on the remote NFS server.

```
Enter remote directory : remote_directory
```

Where: *remote_directory*—Name of the associated directory on your remote server.

The system then prompts you to select a backup mode.

Step 7 Select **P** and press **Enter** to start the partial backup. The system returns a response similar to the following:

```
        Select backup mode: P
a ./ 0 tape blocks
a ./var/ 0 tape blocks
a ./var/log/ 0 tape blocks
.
.
.

backup to va-panthers:/backup/va-blade20000317105337P.tar complete
#
```

The filename on the remote NFS server is the host name of the machine with the date in YYYYMMDDHHMMSS format and “P.tar” appended.

This completes backing up your SC host data to a remote machine. Return to the your chosen upgrade procedure and continue.

Performing a Backup Operation on the Main Memory Database

Use this procedure to store your dial plan data, which is stored in the Main Memory Database (MMDB), in a single file.

Note If your system is *not* configured with a dial plan, do *not* perform this procedure.

Step 1 Change directories to a local subdirectory under the base directory.

For example, enter the following UNIX command to change to the /opt/CiscoMGC/local directory:

```
# cd /opt/CiscoMGC/local
```

Step 2 Run the MMDB backup script by entering the following UNIX command:

```
# ./backupDb.sh filename
```

Where *filename* is the name of the database backup file.

For example, to backup the contents of the MMDB to a file called dplan, you would enter the following command:

```
# ./backupDb.sh dplan
```

The system returns a response similar to the following:

```
Exporting database contents for DSN=howdydb into dplan
The Backup process is being initiated for the datastore howdydb
```

```
Files for /opt/TimesTen32/datastore/howdydb are being backed up onto standard output
Backup Complete
```

CHAPTER 3

Cisco Media Gateway Upgrade Procedures

This chapter describes procedures for upgrading software on Cisco media gateways. It contains the following sections:

- Determining Memory and Software Requirements, page 3-1
- Determining Your Cisco IOS Version, page 3-1
- Upgrading the Cisco AS5300 Universal Access Server, page 3-2
- Upgrading the Cisco AS5350 or Cisco AS5400 Universal Gateway, page 3-4
- Upgrading the Cisco AS5800 Universal Access Server, page 3-6'

Note If your solution uses Cisco Media Gateway Controller Node Manager (CMNM), ensure that the latest CMNM patches are installed before you upgrade media gateways. Go to Cisco Media Gateway Controller Software Center to check for new patches.

Determining Memory and Software Requirements

The amount of memory and appropriate Cisco IOS image depend on the platform and the SS7 Interconnect Solution that the media gateway supports. To determine the latest memory and software requirements, see the following online documents:

- *Release Notes for Cisco SS7 Interconnect for Access Servers Release 2.2(B)*
- *Release Notes for Cisco SS7 Interconnect for Voice Gateways Release 1.3*

Determining Your Cisco IOS Version

To determine the version of Cisco IOS software running on your NAS, log in to the Cisco AS5*X*00 and enter the **show version** EXEC command:

```
AS5300> show version
     Cisco Internetwork Operating System Software
     IOS (tm) 12.1 Software c5300-i-mz, Version 12.1(2), RELEASE SOFTWARE
```

Upgrading the Cisco AS5300 Universal Access Server

The Cisco AS5300 Universal Access Server will not allow the Flash to be overwritten during normal operation. You need to configure the media gateway to boot up from boot Flash (or ROM) so you can copy the upgraded version of Cisco IOS Software into the regular system Flash.

Note In addition to upgrading Cisco IOS, you must also upgrade VCWare on the Cisco AS5300. Refer to the "Upgrading Cisco VCWare" section on page 3-4 for more detailed information.

Blocking Voice Gateway Circuits

Cisco AS5300s that use H.225 Resource Availability Indicator (RAI) to load-share VoIP traffic with other voice gateways require special preparation before you can place them out of service. You must block the appropriate circuits on the Cisco SC2200 and wait for in-progress calls to disconnect on the affected Cisco AS5300. Doing so will cause the NAS to send a "resource unavailable" message to the local H.323 gatekeeper, which will then route calls only to the remaining Cisco AS5300s.

Note This procedure is required only for the Cisco SS7 Interconnect for Voice Gateways Solution in environments where H.225 RAI is used to share egress traffic among multiple Cisco AS5300s.

Complete the following steps before placing the Cisco AS5300 out of service:

Step 1 On the Cisco SC2200, block the circuits that terminate on the NAS.

```
SC2200 mml> blk-cic:point code:CIC=circuit identification code,RNG=CIC+range
```

Step 2 When all in-progress calls have disconnected, disable the loopback interface on the NAS. H.323-id and gatekeeper information is contained in the loopback interface, and disabling this interface will cause the NAS to unregister with the local gatekeeper.

```
AS5300(config)# interface loopback 0
AS5300(config)# shutdown
```

Step 3 Save the configuration of the NAS. This command will prevent the NAS from re-registering with the gatekeeper until Redundant Link Manager (RLM) and all ISDN channels have initialized. The NAS is now ready to be shut down.

```
AS5300# write memory
```

Loading a Cisco IOS Upgrade on the Cisco AS5300

Complete the following steps to upgrade the Cisco IOS Software on a Cisco AS5300:

Step 1 Back up the boot Flash memory.

```
AS5300# copy bootflash tftp
```

Step 2 Back up the Flash memory.

```
AS5300# copy flash tftp
```

Step 3 Back up your configuration. Be sure to use a distinct name for the startup configuration for each of your Cisco AS5300s.

```
AS5300# copy startup-config tftp
```

Step 4 Change the configuration register from its current setting to 0x2101 so that the Cisco AS5300 boots from boot Flash memory. Be sure to enter the **show version** command and take note of the current configuration register settings.

```
AS5300# show version
AS5300# configure terminal
AS5300(config)# config-reg 0x2101
AS5300(config)# exit
AS5300#
```

Step 5 Type **no** when the Cisco AS5300 asks if you want to save the system configuration.

Step 6 Copy the Cisco IOS software to Flash memory.

```
AS5300(boot)# copy tftp flash
```

Step 7 Change the configuration register back to its original setting so that the Cisco AS5300 boots from Flash. In this example, the original setting was 0x2102.

```
AS5300(boot)# configure terminal
AS5300(config)# config-reg 0x2102
AS5300(config)# exit
AS5300(boot)#
```

Step 8 Type **no** when the Cisco AS5300 asks if you want to save the system configuration.

Step 9 Confirm the software upgrade.

```
AS5300# show version
```

Note Complete Step 10 through Step 13 only if your network uses H.225 RAI to load-share VoIP traffic among multiple Cisco AS5300s.

Step 10 Verify that the Redundant Link Manager (RLM) is operational.

```
AS5300# show rlm group 1 status
```

Step 11 Verify that all ISDN channels on the NAS show "maintenance pending."

```
AS5300# show isdn service
```

Step 12 On the Cisco SC2200, unblock the circuits that terminate on the NAS.

```
SC2200 mml> unblk-cic:point code:CIC=circuit identification code,RNG=CIC+range
```

Step 13 Enable the loopback interface on the NAS and define the **h323-gateway voip** parameters. The NAS will re-register with the gatekeeper and begin processing calls.

```
AS5300(config)# interface loopback 0
AS5300(config)# no shut
```

Step 14 If the previous image on your gateway was Cisco IOS 12.2(1c), enter the following commands:

```
AS5300(config)# h323-gateway voip interface
AS5300(config)# h323-gateway voip id gatekeeper-id {ipaddr ip-address [port-number] |
multicast}
```

```
AS5300(config)# h323-gateway voip h323-id interface id
AS5300(config)# h323-gateway voip tech-prefix prefix#
```

Upgrading Cisco VCWare

Cisco VCware is a software image that runs only on voice cards used in the Cisco AS5300. Because Cisco VCWare is a separate image from Cisco IOS Software, it must be loaded and upgraded separately from Cisco IOS Software. For all other Cisco voice gateways using C54x series DSPs, the DSPware is embedded in the Cisco IOS software image, so in those systems, Cisco VCware is not used. For instructions on upgrading Cisco VCWare, refer to *Release Notes for Cisco VCWare on Cisco AS5300 Universal Access Servers* at the following location:

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

Upgrading the Cisco AS5350 or Cisco AS5400 Universal Gateway

Complete the following steps to upgrade the Cisco IOS software on a Cisco AS5350 or Cisco AS5400 universal gateway:

Step 1 Display the contents of Flash memory:

```
Router# cd flash:
Router# dir
Directory of flash:/

1  -rw-     9950528   Jan 01 2000 00:48:59  c5350-js-mz.121-1.XD1.bin

32768000 bytes total (13041600 bytes free)
```

Step 2 Copy the new image from the remote TFTP server into Flash memory. Make sure that you specify your own TFTP server's IP address and Cisco IOS filename. If you encounter issues with upgrading the image, be sure that you can ping the TFTP server and that appropriate directory permissions are configured on the TFTP server. To see the bangs (!) during the download operation, enable line wrap in your terminal emulation software.

Note If you have available space for two images, leave both images in Flash memory. If necessary, you can easily revert back to the previous image. Enter the **boot system flash** *newiosname.***bin** command to point to the new image filename. By default, the first image in Flash memory is loaded.

If you do not have available space, during the copy operation the system displays a message telling you to delete the current file and squeeze the flash to make room for the new image. Enter the **delete flash:***version* command, followed by the **squeeze flash** command, to perform this delete-and-squeeze operation. Then proceed with the copy operation.

```
Router# copy tftp flash
Address or name of remote host [172.22.191.135]? 172.22.191.135
Source filename [c5350-js-mz.121-1.XD1.bin]? c5350-js-mz.121-3.T.bin
Destination filename [c5350-js-mz.121-3.T.bin]?
```

```
Accessing tftp://172.22.191.135/c5350-js-mz.121-3.T.bin...
Loading c5350-js-mz.121-3.T.bin from 172.22.191.135 (via FastEthernet0/0): !!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK - 9775616/19551232 bytes]

9775616 bytes copied in 66.424 secs (148115 bytes/sec)
```

Caution Occasionally TFTP errors occur. Make sure that the verifying checksum reports "OK." Do *not* reload the gateway if the checksum reports errors.

Step 3 Verify that the new image was downloaded. In this example, notice that the Cisco IOS Release 12.1(1)XD image is the first in Flash memory, so it is loaded during the boot sequence. To boot using the new image, you must either delete the unwanted image or use the **boot system** command to specify the alternate image to use during the boot sequence.

```
Router# dir flash:
Directory of flash:/

  1  -rw-     9950528   Jan 01 2000 00:48:59  c5350-js-mz.121-1.XD1.bin
  2  -rw-     9775616   Jan 01 2000 00:59:10  c5350-js-mz.121-3.T.bin

32768000 bytes total (13041600 bytes free)
```

For more information on deleting the image, refer to the document *Cisco IOS File System*, available online at
http://www.cisco.com/univercd/cc/td/doc/product/software/ios113ed/113aa/113aa_2/allplats/ifs.htm

Note The Cisco AS5350 and Cisco AS5400, unlike the Cisco AS5200 and Cisco AS5300, use a Class A Flash File System.

Step 4 To specify the alternate image that is to be used during the boot sequence use the **boot system flash** ***newiosname*.bin** command to specify the location (device) and name of the image to be used:

```
Router(config)# boot system flash c5350-js-mz.121-3.T.bin
Router(config)# ^Z
Router# copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
```

To verify that this command is in effect, use the **show running-configuration** command. Save your running configuration before the reload so that the gateway loads the correct image.

Step 5 Reload the Cisco AS5350 or Cisco AS5400 to run the new image. If you erased the old Cisco IOS image, make sure that the **boot system flash** ***oldiosname*.bin** command is not enabled and pointing to the old image file name; otherwise, the gateway gets stuck trying to reload the old image over and over again.

```
Router# reload
Proceed with reload? [confirm]

System Bootstrap, Version 12.0(20000106:234457) [tombnyg-rommon_1_6 106],
SOFTWARE REV 1.6
Copyright (c) 1994-2000 by cisco Systems, Inc.
AS5400 platform with 131072 Kbytes of main memory
```

```
Self decompressing the image : #################################################
##################################################### [OK]
Self decompressing the image : #################################################
################################################################################
################################################################################
################################################################################
################################################################################
################################################################### [OK]
Press RETURN to get started!
```

Note Most sections of the boot sequence have been omitted from the example.

Tips On system reload, if the console session freezes or displays unusual characters on the screen, you may have a console session mismatch between the Cisco IOS console line speed and the terminal server speed. This mismatch may occur because of the program settings of your console or your terminal server speed.

Upgrading the Cisco AS5800 Universal Access Server

Backing Up Your AS5800 Configuration

Cisco recommends backing up all existing IOS images and configurations from privileged exec mode.

Note Backup current IOS images (boot, router-shelf, dial-shelf), and configurations, to a TFTP server prior to upgrading. By default, files are copied to and from the Cisco TFTP root directory.

Step 1 Backup your existing startup configuration. Use a distinct file name for the startup configuration. This makes it easy to distinguish from other startup configurations previously saved on your TFTP Server.

```
AS5800# copy startup-config tftp
Address or name of remote host []? 171.71.219.167
Destination filename [startup-config]? AS5800-startup
!!
3449 bytes copied in 0.136 secs
```

Step 2 Backup your existing running configuration. Use a distinct file name for the running configuration. This makes it easy to distinguish from other running configurations previously saved on your TFTP Server.

```
AS5800# copy running-config tftp
Address or name of remote host []? 171.71.219.167
Destination filename [running-config]? AS5800-running-config
!!
3312 bytes copied in 0.140 secs
```

Step 3 Save your running-configuration to your startup configuration in NVRAM.

```
Router# copy running-configuration start-up configuration
```

Note Do not modify your running configuration during the IOS upgrade process.

Step 4 Determine the current boot image.

```
AS5800# sh bootflash:
-#- ED --type-- --crc--- -seek-- nlen -length- -----date/time------ name
1   .. image    AC05EDDF  37A6B8   22  3384888 Dec 31 1999 18:08:09 c7200-boot-mz.120-4.XE
```

Step 5 Backup the boot image (c7200-boot-mz.XXX) from bootflash to the TFTP server. Use the file name obtained in Step 4.

```
AS5800# copy bootflash: tftp
Source filename [c]? c7200-boot-mz.120-4.XE
Address or name of remote host []? 171.71.219.167
Destination filename [c7200-boot-mz.120-4.XE]?
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
3384888 bytes copied in 89.920 secs (38032 bytes/sec)
```

Step 6 Determine the router shelf's current flash image.

```
AS5800# sh flash
-#- ED --type-- --crc--- -seek-- nlen -length- -----date/time------ name
1   .. image    AAD4004B  719C50   25  7314384 May 02 2000 13:55:04
c5800-p4-mz_120-4_XL1.bin
```

Step 7 Backup the current router shelf IOS image (C5800-p4-mz.XXX) stored in flash memory. Use the file name obtained in Step 6.

```
AS5800# copy flash tftp
Source filename []? c5800-p4-mz_120-4_XL1.bin
Address or name of remote host []? 171.71.219.167
Destination filename [c5800-p4-mz_120-4_XL1.bin]?
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
7314384 bytes copied in 218.684 secs (33552 bytes/sec)
```

Step 8 On your TFTP Server, verify that files were copied (backed up).

Note By default, files are copied to and from the Cisco TFTP root directory.

Installing New IOS Software on the Cisco AS5800

An AS5800 Cisco IOS upgrade requires a compatible Cisco IOS image upgrade on both the Dial Shelf Controller (DSC) cards and Router Shelf (RS) components of the system. Two distinct upgrade procedures are necessary, one for each component.

Note Cisco recommends upgrading the dial-shelf controller(s) first, since all upgrades are performed through the router shelf. Once DSC(s) are upgraded, the router shelf will not be able to communicate with the DSC(s) until a compatible IOS image is installed on the RS.

Note Do not modify your running configuration during the IOS upgrade process.

Note Upgrade verifications are performed after all necessary upgrades are complete, and all system components are reloaded.

Upgrading the DSC Software

The following procedure outlines commands used to perform a Cisco 5814 Dial Shelf Controller (DSC) software upgrade from the Router Shelf.

Step 1 Login to the AS5800 Router Shelf and enter Enable (privileged exec) mode.

Step 2 Identify IOS images in the DSC bootflash.

```
AS5800# execute-on slot 12 sh bootflash:
DA-Slot12#
-#- ED --type-- --crc--- -seek-- nlen -length- -----date/time------ name
1   .. image    BC8CA85F  251C60   26  2169824 Nov 18 1999 22:12:15
dsc-c5800-mz.120-4.XL1.bin
```

Step 3 Delete the current IOS image(s) from bootflash.

```
AS5800# execute-on slot 12 del bootflash:dsc-c5800-mz.120-4.XL1.bin
DA-Slot12#
Delete filename [dsc-c5800-mz.120-4.XL1.bin]?
Delete bootflash:dsc-c5800-mz.120-4.XL1.bin? [confirm]
AS5800#
```

Step 4 Squeeze the DSC bootflash.

```
AS5800# execute-on slot 12 squeeze bootflash

DA-Slot12#
All deleted files will be removed. Continue? [confirm]
Squeeze operation may take a while. Continue? [confirm]

Squeeze of bootflash complete
```

Step 5 Identify IOS images in the DSC flash.

```
AS5800# execute-on slot 12 sh flash

DA-Slot12#
-#- ED --type-- --crc--- -seek-- nlen -length- -----date/time------ name
1   .. image    BC8CA85F  231C60   26  2169824 Sep 16 1999 18:10:32
dsc-c5800-mz.120-4.XL1.bin
2   .D image    8FDE1F61  45FEC8   18  2286056 Jan 25 2000 18:28:57 dsc-c5800-mz.Jan21
```

Step 6 Delete images or files no longer required.

```
AS5800# execute-on slot 12 delete flash:dsc-c5800-mz.120-4.XL1.bin
DA-Slot12#
Delete filename [dsc-c5800-mz.120-4.XL1.bin]?
Delete slot0:dsc-c5800-mz.120-4.XL1.bin? [confirm]
AS5800#
```

Step 7 Squeeze the DSC flash to remove deleted files.

```
AS5800# execute-on slot 12 squeeze flash:
DA-Slot12#
All deleted files will be removed. Continue? [confirm]
Squeeze operation may take a while. Continue? [confirm]
Writing sector: 1
Squeeze of slot0 complete
```

Step 8 Download the new DSC image from your TFTP server to the DSC flash.

Note By default, files are copied to and from the Cisco TFTP root directory.

```
AS5800# copy tftp:dsc-c5800-mz.120-7.T.bin dsc12-slot0
Address or name of remote host [171.71.219.167]?
Source filename [dsc-c5800-mz.120-7.T.bin ]?
Destination filename [dsc12-slot0]?
Accessing tftp://171.71.219.167/dsc-c5800-mz.120-7.T.bin ...
%Warning: File not a valid executable for this system
Abort Copy? [confirm]n
Loading dsc-c5800-mz.120-7.T.bin from 171.71.219.167 (via FastEthernet0/0/0):
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
```

The following Warning message appears.

```
%Warning: File not a valid executable for this system
Abort Copy? [confirm]
```

Note **Do not abort the copy process.** This message implies that the file being downloaded is not router shelf compatible, which is true. However, the router assumes the file being downloaded will be executed on the router shelf, when, in fact, the file is a dial shelf controller file, being downloaded to the dial shelf through the router, that will ultimately be executed on the dial shelf.

Step 9 Enter “n” to proceed with the download.

Step 10 Copy the new DSC image to the DSC bootflash:

```
AS5800# execute-on slot 12 copy slot0:dsc-c5800-mz.120-7.T.bin
bootflash:
DA-Slot12#
Destination filename [dsc-c5800-mz.120-7.T.bin ]?
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
2169824 bytes copied in 24.464 secs (90409 bytes/sec)
```

Step 11 Reload the DSC to load the new image.

```
Router# execute-on slot 12 reload
```

Step 12 Repeat this procedure if you have a second DSC card to ensure both cards are running the same software release. The only change to the commands will be the slot number (“13” instead of “12”).

Note At this juncture, the DSC(s) and Router Shelf are not running the same IOS image, so you will not be able to communicate with the DSC through the Router Shelf.

Upgrading the Router Shelf Software

The following procedure outlines commands used to perform a Cisco 7206 router shelf (RS) software upgrade from the Router Shelf.

Note Unless you installed new port adapters in the router shelf, do not upgrade the boot image. See Upgrading the Router Shelf Boot Image.

Step 1 Identify IOS images in the RS flash.

```
AS5800# sh flash
-#- ED --type-- --crc--- -seek-- nlen -length- -----date/time------ name
1   .. image    AAD4004B  719C50   25  7314384 May 02 2000 13:55:04
c5800-p4-mz_120-4_XL1.bin
9069488 bytes available (7314512 bytes used)
```

Step 2 Delete images or files no longer required.

```
AS5800# delete slot0:c5800-p4-mz_120-4_XL1.bin
Delete filename [c5800-p4-mz_120-4_XL1.bin]?
Delete slot0:c5800-p4-mz_120-4_XL1.bin? [confirm]
```

Step 3 Squeeze the flash to remove all deleted files.

```
AS5800# squeeze slot0:
All deleted files will be removed. Continue? [confirm]
Squeeze operation may take a while. Continue? [confirm]
Squeeze of slot0 complete
```

Step 4 Download the new image from a TFTP server to the RS flash.

Note By default, files are copied to and from the Cisco TFTP root directory.

```
AS5800# copy tftp:c5800-p4-mz.120-7.T.bin slot0:
Address or name of remote host [171.71.219.167]?
Source filename [c5800-p4-mz.120-7.T.bin ]?
Destination filename [c5800-p4-mz.120-7.T.bin ]?
Accessing tftp://171.71.219.167/c5800-p4-mz.120-7.T.bin ...
Loading c5800-p4-mz.120-7.T.bin from 171.71.219.167 (via
FastEthernet0/0/0):!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
```

Step 5 Upgrade the bootflash, if applicable. See “Upgrading the Router Shelf Boot Image”.

Note Unless you are installing new port adapters in the router shelf, do not upgrade the boot image. See “Upgrading the Router Shelf Boot Image”.

Step 6 Reload the router shelf to load the new image.

```
Router# reload
```

Upgrading the Router Shelf Boot Image

The following procedure outlines commands used to perform a Cisco 7206 router shelf (RS) boot image software upgrade from the router shelf.

Note Unless you installed new port adapters in the router shelf, do not upgrade the boot image.

Step 1 Identify the current bootflash image.

```
AS5800# sh bootflash
-#- ED --type-- --crc--- -seek-- nlen -length- -----date/time------ name
1   .. image    AC05EDDF  37A6B8   22  3384888 Dec 31 1999 18:08:09 c7200-boot-mz.120-4.XE

1 bytes available (3407872 bytes used)
```

Step 2 Delete the current boot image from bootflash.

```
AS5800# del bootflash:
Delete filename []? c7200-boot-mz.120-4.XE
Delete bootflash:c7200-boot-mz.120-4.XE? [confirm]
```

Step 3 Squeeze the bootflash to remove all deleted files.

```
AS5800# squeeze bootflash:
All deleted files will be removed. Continue? [confirm]
Squeeze operation may take a while. Continue? [confirm]

Squeeze of bootflash complete
```

Step 4 Copy the boot image from the TFTP server (c7200-boot-mz.XXX) to bootflash.

```
AS5800# copy tftp bootflash:
Address or name of remote host []? 171.71.219.167
Source filename []? c7200-boot-mz.120-7.T.bin
Destination filename [c7200-boot-mz.120-7.T.bin]?
Accessing tftp://171.71.219.167/c7200-boot-mz.120-7.T.bin...
Loading c7200-boot-mz.120-7.T.bin from 171.71.219.167 (via FastEthernet0/0/0):!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK - 3384888/6769664 bytes]

3384888 bytes copied in 65.112 secs (52075 bytes/sec)
```

Software Upgrade Verification

Perform the following steps to verify the Router Shelf and DSC(s) are running new IOS images, and the Bootflash is running a new boot image.

Step 1 Check the Dial Shelf Controller(s) for a new IOS image.

```
AS5800# execute-on slot 12 show version

DA-Slot12>
Cisco Internetwork Operating System Software
IOS (tm) 5800 Software (C5800-DSC-M), Version 12.0(7)T
TAC:Home:SW:IOS:Specials for info
Copyright (c) 1986-1999 by cisco Systems, Inc.
Compiled Thu 12-Aug-99 18:48 by ayeh
Image text-base: 0x600088F0, data-base: 0x60520000

ROM: System Bootstrap, Version 11.3(1)AA, ROM: 5800 Software (C5800-DSC-M),Version
12.0(7)T

DA-Slot12 uptime is 41 minutes
System returned to ROM by reload
System image file is "slot0:dsc-c5800-mz.120-7.T.bin "

Router# execute-on slot 13 show version (IF APPLICABLE)
```

Step 2 Check the Router Shelf for a new IOS image.

```
AS5800# sh version
Cisco Internetwork Operating System Software
IOS (tm) 5800 Software (C5800-P4-M), Version 12.0(7)T, TAC:Home:SW:IOS:Specials for info
Copyright (c) 1986-1999 by cisco Systems, Inc.
Compiled Thu 12-Aug-99 13:16 by ayeh
Image text-base: 0x60008900, data-base: 0x611A6000

ROM: System Bootstrap, Version 12.0(19990210:195103) [12.7T 105], DEVELOPMENT SOFTWARE
BOOTFLASH: 7200 Software (C7200-BOOT-M), Version 12.0(7)T

doc-rtr58-01 uptime is 9 minutes
System returned to ROM by reload at 16:04:24 CST Fri Jun 9 2000
System restarted at 16:05:39 CST Fri Jun 9 2000
System image file is "slot0:c5800-p4-mz.120-7.T.bin"
```

Step 3 Check the Bootflash for a new boot image.

```
AS5800#sh bootflash:
-#- ED --type-- --crc--- -seek-- nlen -length- -----date/time------ name
1   .. image    AC05EDDF  37A6B8   22  3384888 Jun 12 200014:00:23
c7200-boot-mz.120-7.T.bin

    22856 bytes available (3385016 bytes used)
```

CHAPTER 4

Cisco Signaling Link Terminal Upgrade Procedures

This chapter contains procedures for adding or upgrading Cisco Signaling Link Terminals (SLTs), which is described including the following sections:

- Installing the Cisco SLT Software, page 4-2
- Configuring the Cisco SLT, page 4-2
- Configuring Multiple SLTs, page 4-18
- Upgrading Cisco SLT Software, page 4-19

Note If you are not using Cisco SLTs to terminate signaling links, and are using ITK cards, skip this chapter and proceed to Chapter 6, "Installing the Operating System on the SC Hosts."

For more information, refer to the following documents:

- *Cisco Media Gateway Controller Hardware Installation Guide*—Provides instructions for installing the Cisco SLT hardware. Refer to Chapter 3, "Hardware Installation Instructions."
- *Cisco Media Gateway Controller Software Release 7 Installation and Configuration Guide*—Provides instructions for installing the Cisco SLT software. Refer to Chapter 3, "Installing the Cisco Signaling Link Terminal."
- *Cisco Signaling Link Terminal*—Provides additional information about the Cisco SLT. Available at the following URL:

  http://www.cisco.com/univercd/cc/td/doc/product/access/acs_mod/cis2600/ios_feat/0219nomd.htm
- *Cisco Integrated Signaling Link Terminal* (support for the Cisco SLT on Cisco 5350 and Cisco 5400 platforms)

Note The latest versions of these documents are always posted to Cisco.com. Verify that you have the latest version of the documentation before beginning any procedures.

Installing the Cisco SLT Software

The Cisco 2611 router must be running special Cisco IOS software to function as a Cisco SLT and terminate SS7 signaling links. For information on which Cisco IOS releases can be used in the Cisco SS7 Interconnect for Access Servers and Voice Gateways Solutions, refer to the latest version of the *Release Notes for the Cisco SS7 Interconnect for Access Servers Solution* or *Release Notes for the Cisco SS7 Interconnect for Voice Gateways Solution* (available from your Cisco representative).

Note When used as a Cisco SLT, the Cisco 2611 has SS7 functionality only. All standard Cisco 2611 software features are disabled when running the Cisco SLT image.

To copy a system image from a Trivial File Transfer Protocol (TFTP) server to a Flash memory file system, enter the following command in privileged mode:

```
copy tftp:[[[//location]/directory]/filename] flash-filesystem:[filename]
```

Note For more information about Cisco IOS software, upgrades, and downloading images from the web, see *Cisco SS7 Interconnect for Access Servers and Voice Gateways Solutions Gateway Guide*. See also *Loading and Maintaining System Images and Microcode* at the following url: http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/12cgcr/fun_c/fcprt2/fcimages.htm

Configuring the Cisco SLT

This section contains the following procedures:

- Configuring the Basic Parameters, page 4-2
- Configuring the Physical Interfaces, page 4-5
- Configuring the Session Manager and Reliable User Datagram Protocol, page 4-14

Configuring the Basic Parameters

Note Perform the following steps on each Cisco SLT in your solution.

To configure the basic parameters of the Cisco SLT, complete the following steps:

Step 1 Power on the Cisco SLT:

Note Do not press any keys until the system messages stop. Any keys pressed during this time are interpreted as the first command, which might cause the Cisco SLT to power off and start over. It takes a few minutes for these messages to stop.

Step 2 When the following message appears, enter **y** (yes) to begin the initial configuration dialog:

```
Would you like to enter the initial configuration dialog? [yes/no]: y
```

Tip At any point you may enter a question mark for help. Use **Ctrl-c** to abort configuration dialog at any prompt. Default settings are in square brackets.

Step 3 At the following prompt, type **y** (yes) and press **Enter** to enter basic management setup:

```
Would you like to enter basic management setup? [yes/no]: y
Configuring global parameters:
```

Note Basic management setup provides only enough connectivity for management of the system. Extended setup will ask you to configure each interface on the system.

Step 4 Type the host name for the Cisco SLT and press **Enter**:

```
Enter host name [Router]: router_name
```

Step 5 Type an *enable_secret* password. This password is encrypted for security and cannot be seen in the configuration. The *enable_secret* password is used to protect access to privileged EXEC and configuration modes. After you enter it, *enable_secret* is encrypted in the configuration.

```
Enter enable secret: enable_secret
```

Step 6 Type an *enable_password* that is different from the *enable_secret* password. This password is not encrypted and therefore less secure than the *enable_secret* password, and can be seen in the configuration. The *enable_ password* is used when you do not specify an *enable_secret* password, with some older software versions, and with some boot images.

```
Enter enable password: enable_password
```

Step 7 Type a virtual terminal password (*vt_password*) to prevent unauthenticated access to the Cisco SLT through ports other than the console port. The *vt_password* is used to protect access to the router over a network interface.

```
Enter virtual terminal password: vt_password
```

Step 8 Type **yes** and press **Enter** to begin configuring SNMP parameters:

```
Configure SNMP Network Management? [yes]: yes
            Community string [public]:
```

Step 9 Type the interface name used to connect to the management network and press **Enter**:

```
Current interface summary

Controller Timeslots D-Channel Configurable modes Status
T1 0/2     24        23        pri/channelized    Administratively up
T1 0/3     24        23        pri/channelized    Administratively up

Any interface listed with OK? value "NO" does not have a valid configuration

Interface                  IP-Address      OK? Method Status Protocol
Ethernet0/0                unassigned      NO  unset  up up
Serial0/0                  unassigned      NO  unset  down                  down
Ethernet0/1                unassigned      NO  unset  up                    down
Serial0/1                  unassigned      NO  unset  down                  down

Enter interface name used to connect to the management network from the above interface
summary: Ethernet0/0
```

Step 10 Type **y** and press **Enter** to begin configuring Ethernet interface parameters for the IP address and subnet mask:

```
Configuring interface Ethernet0/0:
Configure IP on this interface? [yes]: y
```

Step 11 Type the IP address and the subnet mask for the Ethernet interface:

```
IP address for this interface: 10.1.1.5
Subnet mask for this interface [255.0.0.0]: 255.255.0.0
Class A network is 10.0.0.0, 16 subnet bits; mask is /16
```

Step 12 Save your configuration to NVRAM and exit the Initial Configuration Mode. The following message text and prompt appears:

```
The following configuration command script was created:

hostname aladdin
enable secret 5 $1$0gLU$vLK1YHrMcianH5oVWFJNP/
enable password lablab
line vty 0 4
password lab
no snmp-server
!
no ip routing
!
interface Ethernet0/0
no shutdown
ip address 10.1.1.5 255.255.0.0
!
interface Serial0/0
shutdown
no ip address
!
interface Ethernet0/1
shutdown
no ip address
!
interface Serial0/1
shutdown
no ip address
!
end

[0] Go to the IOS command prompt without saving this config.
[1] Return back to the setup without saving this config.
[2] Save this configuration to nvram and exit.
Enter your selection [2]: 2
Building configuration...
Use the enabled mode 'configure' command to modify this configuration.

Press RETURN to get started!
```

Step 13 If you do not see a # prompt at the end of the text, press **Enter**.

Step 14 At the command prompt, type each of the following commands and press **Enter** to access global configuration mode:

```
enable password
config t
```

This completes the basic Cisco SLT configuration. Continue to the next section to configure the physical interfaces.

Configuring the Physical Interfaces

This section contains the following procedures:

- Configuring the T1/E1 Multiflex Trunk Interfaces, page 4-5
- Configuring Drop and Insert, page 4-8
- Verifying T1/E1 Multiflex Trunk Interface Configuration, page 4-9
- Configuring the Serial Interfaces, page 4-12
- Configuring the Ethernet Interface, page 4-12
- Verifying the Ethernet Interface Configuration, page 4-13
- Verifying the Session Manager and RUDP Configuration, page 4-15
- Configuring the MTP2 Variant, page 4-17

Configuring the T1/E1 Multiflex Trunk Interfaces

The T1/E1 multiflex trunk interface cards are dual-mode T1 or E1 interfaces in a VWIC (Voice/WAN Interface Card) form for voice, data, and integrated voice/data applications. They support the SS7 Cisco SLT function, as do serial WICs.

The T1/E1 VWIC supports the following T1/E1 functionality:

- Single or dual port, structured or unstructured T1/E1 functionality
- Drop and Insert (also called TDM Cross-Connect) between the T1/E1 ports on dual-port cards, used to hairpin bearer channels to a media gateway device and allow the interchange of time-division multiplexing (TDM) slots between the ports on a two-port card
- Physical layer alarm forwarding between the two E1/T1 ports on dual-port cards

For additional information about the T1/E1 multiflex trunk interface cards and configuring other types of WICs, see *Cisco WAN Interface Cards Hardware Installation Guide*.

Note For serial WICs, no particular configuration is required, except to ensure that the interfaces are not shut down.

To configure the T1/E1 multiflex trunk interfaces of the Cisco SLT, complete the following steps:

Step 1 To start global configuration mode, type the following command and press **Enter**:

```
Router# configure terminal
```

Step 2 To start controller configuration mode for the T1 controller at the specified *slot/port* location, type the following command and press **Enter**:

```
Router(config)# controller {T1 | E1} 0/port
```

Where:

- The value for slot is always 0.

- The port value can be a number 0 through 3.

Note For information about WAN interface slot and port numbering, see *Cisco WAN Interface Cards Hardware Installation Guide.*

Step 3 To set framing, type one of the following commands (for either T1 or E1) and press **Enter**:

T1 Interface	E1 Interface
`Router(config-controller)# `**`framing esf`**	`Router(config-controller)# `**`framing crc4`**

Step 4 To set line coding, type one of the following commands (for either T1 or E1) and press **Enter**:

T1 Interface	E1 Interface
`Router(config-controller)# `**`linecode b8zs`**	`Router(config-controller)# `**`linecode hdb3`**

Note The settings above are the most common settings. Consult your service provider and *Wide Area Network Configuration Guide* for more information.

Step 5 This command specifies the impedance (amount of wire resistance and reactivity to current) for the E1 termination. Impedance levels are maintained to avoid data corruption over long-distance links. To enter a line-termination value for an E1 link, type one of the following commands and press **Enter**:

T1 Interface	E1 Interface
This parameter is for E1 interfaces, only.	Router(config-controller)# **line-termination {75-ohm | 120-ohm}** • Specify 120-ohm to match the balanced 120-ohm interface. This is the default. • Specify 75-ohm for an unbalanced BNC 75-ohm interface.

Step 6 To set the cable length, type one of the following commands and press **Enter**:

<table>
<tr><th>T1 Interface</th><th>E1 Interface</th></tr>
<tr><td>• To set a cable length longer than 655 feet, type the following command and press <b>Enter</b>, using the appropriate parameters as shown below:
Router(config-controller)# <b>cablelength long {gain26 | gain36} {-15db | -22.5db | -7.5db | 0db}</b>
– <b>gain26</b>—Specifies the decibel pulse gain at 26. This is the default pulse gain.
– <b>gain36—</b>Specifies the decibel pulse gain at 36.
– <b>-15db—</b>Specifies the decibel pulse rate at -15 decibels.
– <b>-22.5db—</b>Specifies the decibel pulse rate at -22.5 decibels.
– <b>-7.5db—</b>Specifies the decibel pulse rate at -7.5 decibels.
– <b>0db—</b>Specifies the decibel pulse rate at 0 decibels. This is the default pulse rate.
• To set a cable length 655 feet or shorter, type the following command and press <b>Enter</b>, using the appropriate parameters as shown below:
Router(config-controller)# <b>cablelength short {133 | 266 | 399 | 533 | 655}</b>
– <b>133—</b>Specifies a cable length from 0-133 feet.
– <b>266—</b>Specifies a cable length from 134-266 feet.
– <b>399</b>—Specifies a cable length from 267-399 feet.
– <b>533</b>—Specifies a cable length from 400-533 feet.
– <b>655</b>—Specifies a cable length from 534-655 feet.
<b>Note</b> If you do not set the cable length, the system defaults to a setting of <b>cablelength long gain26 0db</b>.</td><td>This parameter is for T1 interfaces, only.</td></tr>
</table>

Step 7 Specify the channel group and time slots to be mapped. Channel group 0 or 1 can be configured. Generally, only one time slot is configured when you are using the Cisco SLT feature, as is shown in this example where time slot 24 is used for a T1 interface and time slot 16 is used for an E1 interface. A channel group creates a virtual serial interface. It is designated *slot*/*port*:*subinterface*, as follows:

- *slot* is the slot location of the WIC/VWIC where the channel group was created (0 or 1).
- *port* is the WIC/VWIC port address (a number from 0 through 3)
- *subinterface* is the channel group number (0 or 1)

To specify the channel group and time slots to be mapped, type one of the following commands and press **Enter**:

T1 Interface	E1 Interface
`Router(config-controller)# channel-group 0 timeslots 24`	`Router(config-controller)# channel-group 0 timeslots 16`

Step 8 If necessary, repeat Step 2 through Step 7 to configure the remaining Cisco SLT interfaces.

Step 9 To exit controller configuration mode, type the following command and press **Enter**:

```
Router(config-controller)# exit
```

Configuring Drop and Insert

To configure Drop and Insert (the TDM cross-connect function), complete the following steps:

Step 1 To begin global configuration mode, type the following command and press **Enter**:

```
Router# configure terminal
```

Step 2 To begin controller configuration mode for the T1 controller at the specified *slot/port* location, type the following command and press **Enter**:

```
Router(config)# controller {T1 | E1} 0/port
```

Where:

- The value for *slot* is always 0.
- The *port* value is a number from 0 through 3.

Note For information about WAN interface slot and port numbering, see *Cisco WAN Interface Cards Hardware Installation Guide.*

Step 3 Enter this command to create TDM channel groups for the Drop-and-Insert function with a two-port T1 or E1 multiflex trunk interface card. You must set up a TDM group for each interface that you wish to cross-connect. To create TDM channel groups, type the following command and press **Enter**:

```
Router(config-controller)# tdm-group tdm-group-no timeslots timeslot-list
```

Where:

- *tdm-group-no* is a value from 1 through 31 that identifies the channel group. Group numbers for controller groups must be unique. For example, a TDM group should not have the same ID number as a channel group.
- *timeslot-list* is a single number, numbers separated by commas, or a pair of numbers separated by a hyphen to indicate a range of time slots. For T1, allowable values are 1 through 24. For E1, allowable values are 1 through 31.

Note You must set up a TDM group for each interface that you wish to cross-connect.

Step 4 To activate the controller, type the following command and press **Enter**:

```
Router(config-controller)# no shutdown
```

Step 5 Repeat Step 3 and Step 4 for the second interface.

Step 6 To exit controller configuration mode, type the following command and press **Enter**:

```
Router(config-controller)# exit
```

Step 7 To establish the connection between two T1 or E1 TDM groups of time slots on the trunk interface, type the following command and press **Enter**:

```
Router(config)# connect id T1 slot/port tdm-group-no-1 T1 slot/port tdm-group-no-2
```

Where:

- *id* is a name for the connection.
- Each T1 controller is identified by its *slot/port* location:
  - The *slot* value is always 0.
  - The *port* value can be a number from 0 through 3.
- *tdm-group-no-1* and *tdm-group-no-2* identify the TDM group numbers (1 through 31) on the specified controller. (You already set up groups in Step 3.)

Step 8 To exit global configuration mode, type the following command and press **Enter**:

```
Router(config)# exit
```

Verifying T1/E1 Multiflex Trunk Interface Configuration

To verify the initial T1/E1 trunk interface configuration, complete the following steps:

Step 1 Enter the privileged EXEC **show controllers t1** or **show controllers e1** command; for example, **show controllers e1** or **show controllers t1**.

Following is sample output from both commands. Important information appears in bold:

```
Router# show controllers e1
E1 0/2 is up.
  Applique type is Channelized E1 - balanced
  Cablelength is Unknown
  No alarms detected.
  Version info Firmware: 19990702, FPGA: 6
  Framing is CRC4, Line Code is HDB3, Clock Source is Line.
  Data in current interval (599 seconds elapsed):
     0 Line Code Violations, 0 Path Code Violations
     0 Slip Secs, 0 Fr Loss Secs, 0 Line Err Secs, 0 Degraded Mins
     0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs, 0 Unavail Secs
  Total Data (last 10 15 minute intervals):
     435334 Line Code Violations, 1 Path Code Violations,
     8 Slip Secs, 69 Fr Loss Secs, 9 Line Err Secs, 0 Degraded Mins,
     8 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs, 69 Unavail Secs
E1 0/3 is down.
  Applique type is Channelized E1 - balanced
  Cablelength is Unknown
  Far End Block Errors Detected
  Receiver has loss of signal.
  Version info Firmware: 19990702, FPGA: 6
  Framing is CRC4, Line Code is HDB3, Clock Source is Line.
  Data in current interval (602 seconds elapsed):
     0 Line Code Violations, 0 Path Code Violations
     0 Slip Secs, 602 Fr Loss Secs, 0 Line Err Secs, 0 Degraded Mins
     0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs, 603 Unavail Secs
  Total Data (last 10 15 minute intervals):
     0 Line Code Violations, 0 Path Code Violations,
     0 Slip Secs, 9000 Fr Loss Secs, 0 Line Err Secs, 0 Degraded Mins,
     0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs, 9000 Unavail Secs
```

```
Router# show controllers t1
T1 0/0 is up.
  Applique type is Channelized T1
  Cablelength is short 133
  No alarms detected.
  Version info Firmware: 19990702, FPGA: 6
  Framing is ESF, Line Code is B8ZS, Clock Source is Line.
  Data in current interval (608 seconds elapsed):
     136066 Line Code Violations, 778727 Path Code Violations
     567 Slip Secs, 0 Fr Loss Secs, 608 Line Err Secs, 0 Degraded Mins
     0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs, 608 Unavail Secs
  Total Data (last 10 15 minute intervals):
     4286812 Line Code Violations, 11478885 Path Code Violations,
     7734 Slip Secs, 69 Fr Loss Secs, 8996 Line Err Secs, 0 Degraded Mins,
     0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs, 9000 Unavail Secs
```

Step 2 To view channel groups configured as virtual serial interfaces, type the **show interface serial** *slot*/*port*:*subinterface* command and press **Enter**:

```
Router# show interface serial 0/0:0
```

The following text appears:

```
Serial0/0:0 is reset, line protocol is down
  Hardware is PowerQUICC Serial
  MTU 1500 bytes, BW 56 Kbit, DLY 20000 usec,
     reliability 253/255, txload 1/255, rxload 1/255
  Encapsulation SS7 MTP2, loopback not set
  Keepalive set (10 sec)
  Last input never, output 00:12:22, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0 (size/max/drops); Total output drops: 0
  Queueing strategy: weighted fair
  Output queue: 0/1000/64/0 (size/max total/threshold/drops)
     Conversations  0/0/256 (active/max active/max total)
     Reserved Conversations 0/0 (allocated/max allocated)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     0 packets input, 0 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     1437 input errors, 2 CRC, 31 frame, 0 overrun, 0 ignored, 1404 abort
     128055 packets output, 512220 bytes, 0 underruns
     0 output errors, 0 collisions, 2 interface resets
     0 output buffer failures, 0 output buffers swapped out
     1 carrier transitions
  Timeslot(s) Used:1, Transmitter delay is 0 flags
```

Step 3 To view information about the virtual serial interface, type the **show controllers serial** *slot*/*port*:*subinterface* command and press **Enter**:

```
Router# show controllers serial 0/2:0
```

The following text appears:

```
Interface Serial0/2:0
Hardware is PowerQUICC MPC860idb at 0x81143590, driver data structure at 0x81145
474
SCC Registers:
General [GSMR]=0x2:0x00000033, Protocol-specific [PSMR]=0x8
Events [SCCE]=0x0200, Mask [SCCM]=0x001F, Status [SCCS]=0x02
Transmit on Demand [TODR]=0x0, Data Sync [DSR]=0x7E7E
Interrupt Registers:
Config [CICR]=0x00367F80, Pending [CIPR]=0x04000246
Mask   [CIMR]=0x60240000, In-srv  [CISR]=0x00000000
Command register [CR]=0xD40
Port A [PADIR]=0x00F0, [PAPAR]=0x25F0
       [PAODR]=0x0000, [PADAT]=0x5A4F
Port B [PBDIR]=0x0000F, [PBPAR]=0x0000E
       [PBODR]=0x00000, [PBDAT]=0x37FFD
Port C [PCDIR]=0x00C, [PCPAR]=0xA00
       [PCSO]=0x000,  [PCDAT]=0x5F2, [PCINT]=0xFFF
Receive Ring
        rmd(68012930): status 9000 length 6 address 2DA22E4
        rmd(68012938): status 9000 length 6 address 2DA3AA4
        rmd(68012940): status 9000 length 6 address 2DA1E24
        rmd(68012948): status 9000 length 6 address 2DA27A4
        rmd(68012950): status 9000 length 6 address 2DA5724
        rmd(68012958): status 9000 length 6 address 2DA14A4
        rmd(68012960): status 9000 length 6 address 2DA5264
        rmd(68012968): status 9000 length 6 address 2DA4684
        rmd(68012970): status 9000 length 6 address 2DA4424
        rmd(68012978): status 9000 length 6 address 2DA1964
        rmd(68012980): status 9000 length 6 address 2DA4B44
        rmd(68012988): status 9000 length 6 address 2DA60A4
        rmd(68012990): status 9000 length 6 address 2DA2544
        rmd(68012998): status 9000 length 6 address 2DA3124
        rmd(680129A0): status 9000 length 6 address 2DA0FE4
        rmd(680129A8): status B000 length 6 address 2DA3844
Transmit Ring
        tmd(680129B0): status DC00 length 4 address 2AD9EA8
        tmd(680129B8): status DC00 length 4 address 2AD7568
        tmd(680129C0): status DC00 length 4 address 2ADA428
        tmd(680129C8): status DC00 length 4 address 2ADA6E8
        tmd(680129D0): status DC00 length 4 address 2AD7DA8
        tmd(680129D8): status DC00 length 4 address 2AD5468
        tmd(680129E0): status DC00 length 4 address 2AD8328
        tmd(680129E8): status DC00 length 4 address 2AD85E8
        tmd(680129F0): status DC00 length 4 address 2AD5CA8
        tmd(680129F8): status CE00 length 4 address 2AD8B68
        tmd(68012A00): status DC00 length 4 address 2AD8E28
        tmd(68012A08): status DC00 length 4 address 2AD64E8
        tmd(68012A10): status DC00 length 4 address 2AD67A8
        tmd(68012A18): status DC00 length 4 address 2AD9668
        tmd(68012A20): status DC00 length 4 address 2AD9928
        tmd(68012A28): status FC00 length 4 address 2AD6FE8
SPI Mode [SPMODE]=0xF70, Events [SPIE]=0x0
    Mask [SPIM]=0x0, Command [SPCOM]=0x0
SI Mode [SIMODE]=0x80408040, Global [SIGMR]=0xE
   Cmnd [SICMR]=0x0, Stat [SISTR]=0x0
SI Clock Route [SICR]=0x00004040
```

```
SCC GENERAL PARAMETER RAM (at 0x68013D00)
Rx BD Base [RBASE]=0x2930, Fn Code [RFCR]=0x18
Tx BD Base [TBASE]=0x29B0, Fn Code [TFCR]=0x18
Max Rx Buff Len [MRBLR]=1548
Rx State [RSTATE]=0x0, BD Ptr [RBPTR]=0x2970
Tx State [TSTATE]=0x188920A3, BD Ptr [TBPTR]=0x2A08

SCC SS7 PARAMETER RAM (at 0x68013D38)
CRC Preset [C_PRES]=0xFFFF, Mask [C_MASK]=0xF0B8
Error-free SUs [EFSUC] = 22927
Max frm len [MFLR] = 278
Erm [ERM] = 0x0,N [NOCTETS] = 16, N_cnt [NOCTETS_CNT] = 12, T [ERM_THRESH] = 64,
 D [ERM_EFSUS] = 256, D_cnt [ERM_EFSUS_CNT] = 97
SS7 options [SS7_OPT] = 0x10F
Filter masks [MASK1] = 0xFFFFFFFF, [MASK2] = 0xFF

buffer size 1524
PQUICC SCC specific errors:
0 input aborts on receiving flag sequence
0 throttles, 0 enables
0 overruns
0 transmitter underruns
0 transmitter CTS losts
```

Configuring the Serial Interfaces

To configure the 1T and 2T serial interfaces, complete the following steps:

Step 1 To begin global configuration mode, type the following command and press **Enter**:

```
Router# configure terminal
```

Step 2 To begin interface configuration mode for the serial interface, type the following command and press **Enter**:

```
Router(config)# interface serial 0/2
```

Step 3 To activate the interface, type the following command and press **Enter**:

```
Router(config-if)# no shutdown
```

Step 4 To exit serial interface configuration mode, type the following command and press **Enter**:

```
Router(config-if)# exit
```

Configuring the Ethernet Interface

The Cisco SLT uses the built-in Ethernet interface for connection to the IP network that backhauls SS7 signaling between the Cisco SLT and the SC host.

To configure the Ethernet interface, complete the following steps:

Step 1 To begin global configuration mode, type the following command and press **Enter**:

```
Router# configure terminal
```

Step 2 To begin interface configuration mode for the built-in Ethernet interface, type the following command and press **Enter**:

```
Router(config)# interface Ethernet 0/0
```

Step 3 To assign an IP address and subnet mask to the interface, type the following command and press **Enter**:

```
Router(config-if)# ip address 10.10.11.1 255.255.255.0
```

Step 4 To activate the interface, type the following command and press **Enter**:

```
Router(config-if)# no shutdown
```

Step 5 To exit interface configuration mode, type the following command and press **Enter**:

```
Router(config-if)# exit
```

Verifying the Ethernet Interface Configuration

To verify the Ethernet interface configuration, type the **show interface ethernet 0/0** privileged EXEC command at the **Router #** prompt and press **Enter**:

```
Router# show interface ethernet 0/0
```

The following verification text appears:

```
Ethernet0/0 is up, line protocol is up
  Hardware is AmdP2, address is 0050.7337.5100 (bia 0050.7337.5100)
  Internet address is 255.251.111.6/24
  MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:00, output 00:00:00, output hang never
  Last clearing of "show interface" counters 10:00:36
  Queueing strategy: fifo
  Output queue 0/40, 0 drops; input queue -196/75, 0 drops
  5 minute input rate 3000 bits/sec, 5 packets/sec
  5 minute output rate 2000 bits/sec, 4 packets/sec
     45891 packets input, 3234949 bytes, 0 no buffer
     Received 1593 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 input packets with dribble condition detected
     61546 packets output, 3728838 bytes, 0 underruns(518/2091/0)
     0 output errors, 2609 collisions, 3 interface resets
     0 babbles, 0 late collision, 875 deferred
     0 lost carrier, 0 no carrier
     0 output buffer failures, 0 output buffers swapped out
```

This completes the physical interface configuration. Continue to the next section ("Configuring the Session Manager and Reliable User Datagram Protocol") to configure the Session Manager, RUDP, and the variant.

Configuring the Session Manager and Reliable User Datagram Protocol

The Session Manager and the Reliable User Datagram Protocol (RUDP) are responsible for managing the communication sessions with the SC hosts. Regardless of the number of SS7 links that the SC host activates on the Cisco SLT, the router maintains only one Session Manager session with each SC host.

Note You must reboot the Cisco SLT after setting a new session configuration or after changing an existing session configuration. Do not change session timers unless instructed to do so by Cisco technical support. Changing timers might result in service interruption or outage.

To configure the session for establishing communications with the SC host, complete the following steps:

Note You can define either one or two sessions.

Step 1 To begin global configuration mode, type the following command and press **Enter**:

```
Router# configure terminal
```

Step 2 To set the switchover (failover) timer, type the following command and press **Enter**:

```
Router(config)# ss7 set failover-timer 5
```

Note When an active session fails, the failover-timer value specifies the number of seconds that the Session Manager waits for the active session to recover, or for the standby SC host to indicate that the Cisco SLT should switch traffic to the standby session and make that session the active session. If the timer expires without a recovery of the original session or an active message from the standby SC host, the signaling links are taken out of service. The default setting is 3 seconds, and values from 1 through 10 are valid.

Step 3 Specify the remote four-part IP address and the remote UDP port first, then the local IP address and UDP port, by typing in the following command and pressing **Enter**:

```
ss7 session-session number {address remote-address remote-port local-address local-port}
```

where *session number* is either 1 or 0.

Step 4 To configure the address pairs and ports for the first Session Manager session, type the following command and press **Enter**:

```
Router(config)# ss7 session-0 address 10.0.0.1 7000 10.0.0.2 7000
```

Note There are two sessions: one for the active SC host and one for the standby SC host. The port numbers that each SC use to communicate with the Cisco SLT must be unique for the active and standby machines and must match the settings for *.stPort in the XECfgParm.dat file.

Step 5 To configure the address pairs and ports for the second Session Manager session, type the following command and press **Enter**:

```
Router(config)# ss7 session-0 address 10.0.0.1 7001 10.0.0.2 7001
```

Note You can specify any UDP port greater than 1024.

Step 6 To exit interface configuration mode, type the following command and press **Enter**:

```
Router(config-if)# exit
```

Step 7 To save the new configuration as the startup configuration, type the following command and press **Enter**:

```
Router# copy system:running-config nvram:startup-config
```

Step 8 To reload the Cisco SLT, type the following command and press **Enter**:

```
Router# reload
```

Note You must reload the Cisco SLT if you delete a session or modify any of the parameters of a session. For a complete list of SS7 parameters and Cisco SLT commands, see the Appendix A of the *Cisco Media Gateway Controller Software Release 7 Installation and Configuration Guide.*

Verifying the Session Manager and RUDP Configuration

To verify the Session Manager and RUDP configuration, complete the following steps:

Step 1 To view a session configuration, type the privileged EXEC **show ss7 sm session** command, with or without a session number of 0 or 1, and press **Enter**:

```
Router# show ss7 sm session
Session[0]: Remote Host 255.251.250.252:8060, Local Host 255.251.251.252:8060
      retrans_t = 600
      cumack_t  = 300
      kp_t      = 2000
      m_retrans = 2
      m_cumack  = 3
      m_outseq  = 3
      m_rcvnum  = 32

Session[1]: Remote Host 255.251.250.253:8060, Local Host 255.251.251.252:8061
      retrans_t = 600
      cumack_t  = 300
      kp_t      = 2000
      m_retrans = 2
      m_cumack  = 3
      m_outseq  = 3
      m_rcvnum  = 32
```

Step 2 To verify the switchover (failover) timer setting, type the privileged EXEC **show ss7 sm set** command and press **Enter**:

```
Router# show ss7 sm set
Session Manager Set
      failover timer = 3 seconds
```

Step 3 To view Session Manager statistics, type the privileged EXEC **show ss7 sm stats** command and press **Enter**:

```
Router# show ss7 sm stats
```

Note You can specify a session number of 1 or 2.

The following text appears:

```
Router# show ss7 sm stats

-------------------- Session Manager  --------------------

Session Manager state             = SESSION SET STATE-ACTIVE
Session Manager Up count          = 1
Session Manager Down count        = 0
   lost control packet count      = 0
              lost PDU count      = 0
 failover timer expire count      = 0
 invalid_connection_id_count      = 0

Session[0] statistics  SM SESSION STATE-STANDBY:
Session Down count               = 0
   Open Retry count              = 0

   Total Pkts receive count      = 1
   Active Pkts receive count     = 0
   Standby Pkts receive count    = 1
   PDU Pkts receive count        = 0
   Unknown Pkts receive count    = 0

   Pkts send count               = 0
   Pkts requeue count            = 0
    -Pkts window full count      = 0
    -Pkts resource unavail count = 0
    -Pkts enqueue fail count     = 0
   PDUs dropped (Large)          = 0
   PDUs dropped (Empty)          = 0

   RUDP Not Ready Errs           = 0
   RUDP Connection Not Open      = 0
   RUDP Invalid Conn Handle      = 0
   RUDP Unknown Errors           = 0
   RUDP Unknown Signal           = 0
   NonActive Receive count       = 0

Session[1] statistics  SM SESSION STATE-ACTIVE:
Session Down count               = 0
   Open Retry count              = 0

   Total Pkts receive count      = 2440
   Active Pkts receive count     = 1
   Standby Pkts receive count    = 0
   PDU Pkts receive count        = 2439
   Unknown Pkts receive count    = 0

   Pkts send count               = 2905
   Pkts requeue count            = 0
    -Pkts window full count      = 0
    -Pkts resource unavail count = 0
    -Pkts enqueue fail count     = 0
   PDUs dropped (Large)          = 0
   PDUs dropped (Empty)          = 0
   RUDP Not Ready Errs          = 0
   RUDP Connection Not Open     = 0
   RUDP Invalid Conn Handle     = 0
   RUDP Unknown Errors          = 0
   RUDP Unknown Signal          = 0
   NonActive Receive count      = 0
```

Configuring the MTP2 Variant

SS7 MTP2 supports the following four variants:

- Telcordia (formerly Bellcore)
- ITU
- TTC (Japan Telecom)

Parameters in one variant have different meanings, purposes, and ranges in another variant. See Appendix A of the *Cisco Media Gateway Controller Software Release 7 Installation and Configuration Guide* for more on MTP 2 variant commands and their parameters.

Pay attention to the following:

- Parameters that are not configured remain at their default values.
- The channel to be configured must be out of service at the SC host before you can change the variant or the variant configuration.
- Once variant configuration changes have been made, you must reload the Cisco SLT to apply them.

To configure the MTP2 variant, complete the following steps:

Step 1 To begin global configuration mode, type the following command and press **Enter**:

```
Router# configure terminal
```

Step 2 To set the amount of DRAM to be used for I/O memory to 40 percent, type the following command and press **Enter**:

```
Router(config)# mem iomem 40
```

Note You must set the I/O memory to at least 40 percent in order to have enough memory for the SS7 MTP2 signaling.

Step 3 To configure the MTP2 variant Telcordia (formerly Bellcore) for channel 2, type the following command and press **Enter**:

```
Router(config)# ss7 mtp2-variant Bellcore 2
```

Step 4 To set the aligned timer to 30,000 milliseconds, type the following command and press **Enter**:

```
Router(config-Bellcore)# T3 30000
```

Step 5 To set the maximum number of message signal units (MSUs) waiting for acknowledgment to 16, type the following command and press **Enter**:

```
Router(config-Bellcore)# unacked-MSUs 16
```

Step 6 To set the excessive delay timer to 50,000 milliseconds, type the following command and press **Enter**:

```
Router(config-Bellcore)# T7 50000
```

Step 7 To exit Bellcore variant configuration mode, type the following command and press **Enter**:

```
Router(config-Bellcore)# exit
```

Step 8 To exit configuration mode, type the following command and press **Enter**:

```
Router(config-if)# end
```

Step 9 To save the running configuration to startup configuration, type the following command and press **Enter**:

```
Router# copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
```

Configuring Multiple SLTs

To configure the second SLT in a pair, complete the following steps:

Step 1 Repeat the above procedure for Configuring the Cisco SLT, page 4-2, beginning at step 1.

Make sure that you assign unique IP addresses, UDP port numbers based on the local UDP port number of a session, and the remote UDP port number.

Example

If your provisioning file on the active SC2200 has the following line:

```
prov-add:c7iplnk:name="link1-1",if="en0",ipaddr="IP_Addr1",port=7002,
peeraddr="172.24.233.194",peerport=7000,lnkset="ls4",timeslot=1,slc=0
```

and the active system and standby system have the following IP addresses:

active system:172.24.233.227

standby system:172.24.233.228

then the configuration for SLT (172.24.233.194) would be as follows:

```
ss7 session-0 address 172.24.233.227 7002 172.24.233.194 7000
ss7 session-1 address 172.24.233.228 7002 172.24.233.194 7001
```

Note One SLT can terminate SS7 links from one OPC only.

Step 2 If your configuration contains additional Cisco SLTs, you must repeat Step 1 for each SLT, again using unique IP addresses, and assigning UDP port numbers based on the local UDP port number of a session and the remote UDP port number.

Upgrading Cisco SLT Software

This section includes the following procedures:

- Determining Memory and Software Requirements, page 4-19
- Determining Your Cisco IOS Version, page 4-19
- Upgrading Cisco IOS Software, page 4-19

Determining Memory and Software Requirements

The amount of memory and appropriate Cisco IOS image depend on the platform and the SS7 Interconnect Solution that the media gateway supports. To determine the latest memory and software requirements see the following online documents:

- *Release Notes for Cisco SS7 Interconnect for Access Servers Release 2.2(B)*
- *Release Notes for Cisco SS7 Interconnect for Voice Gateways Release 1.3*
- *Release Notes for the Cisco Signaling Link Terminal*

Determining Your Cisco IOS Version

To determine the version of Cisco IOS software running on your Cisco SLT, log in and enter the **show version** EXEC command:

```
SLT> show version
     Cisco Internetwork Operating System Software
     IOS (tm) 12.1 Software c2600-ipss7-mz, Version 12.1(2), RELEASE SOFTWARE
```

Upgrading Cisco IOS Software

Complete the following steps to upgrade the Cisco IOS Software on a Cisco SLT:

Step 1 Back up the boot Flash memory.

```
SLT# copy bootflash tftp
```

Step 2 Back up the Flash memory.

```
SLT# copy flash tftp
```

Step 3 Back up your configuration. Be sure to use a distinct name for the startup configuration for each of your Cisco SLTs.

```
SLT# copy startup-config tftp
```

Step 4 Copy the new Cisco IOS image to Flash memory.

```
SLT(boot)# copy tftp flash
```

Step 5 Reload the Cisco SLT.

```
SLT(boot)# reload
```

Step 6 Confirm the software upgrade.

```
SLT# show version
```

CHAPTER 5

Upgrading SC Host Hardware

You may need to upgrade SC host hardware components to comply with the current hardware requirements listed in "SC Host Minimum Server Requirements" section on page 1-17. This chapter presents instructions for upgrading common hardware components.

Warning **Only trained and qualified personnel should be allowed to install, replace, or service this equipment.**

Caution You must back up your data before performing any hardware upgrades. See Chapter 2, "Backing Up Your SC Host Data" for instructions on backing up your data.

Note This document presents edited information from the Sun hardware manuals. For the latest and most complete information, see the hardware documentation that shipped with your product.

This chapter includes the following sections:

- Upgrading Your Hardware, page 5-1
- Verifying The Hardware Installation, page 5-18

Upgrading Your Hardware

There are three server platforms supported for use as an SC host:

- Sun Netra t100/105 (simplex configurations only)
- Sun Netra t 1120/1125
- Sun Netra t 1400/1405

This sections contains procedures for upgrading common hardware components and guidelines for performing the upgrades for each of these servers. This information is found in the following sections:

- Required Tools, page 5-2
- Upgrading Hard Drives, page 5-2
- Upgrading Processors, page 5-7
- Upgrading Memory, page 5-11

Required Tools

You will need the following tools to perform the procedures in these sections:

- No.1 and No.2 Phillips-head screwdriver
- Needle-nose pliers (Netra t 1120/1125 only)
- Antistatic wrist strap
- Digital voltage meter (DVM)
- Riser card torque tool (Netra t 1400/1405 only)
- Antistatic mat—Place ESD-sensitive components such as disk drives and memory modules on an antistatic mat. The following items can be used as an antistatic mat:
  - Bag used to wrap a Sun replacement part
  - Shipping container used to package a Sun replacement part
  - Inner side (metal part) of the system unit cover
  - Sun ESD mat, part number 250-1088 (which can be purchased through your Sun sales representative)
  - Disposable ESD mat; shipped with replacement parts or optional system features

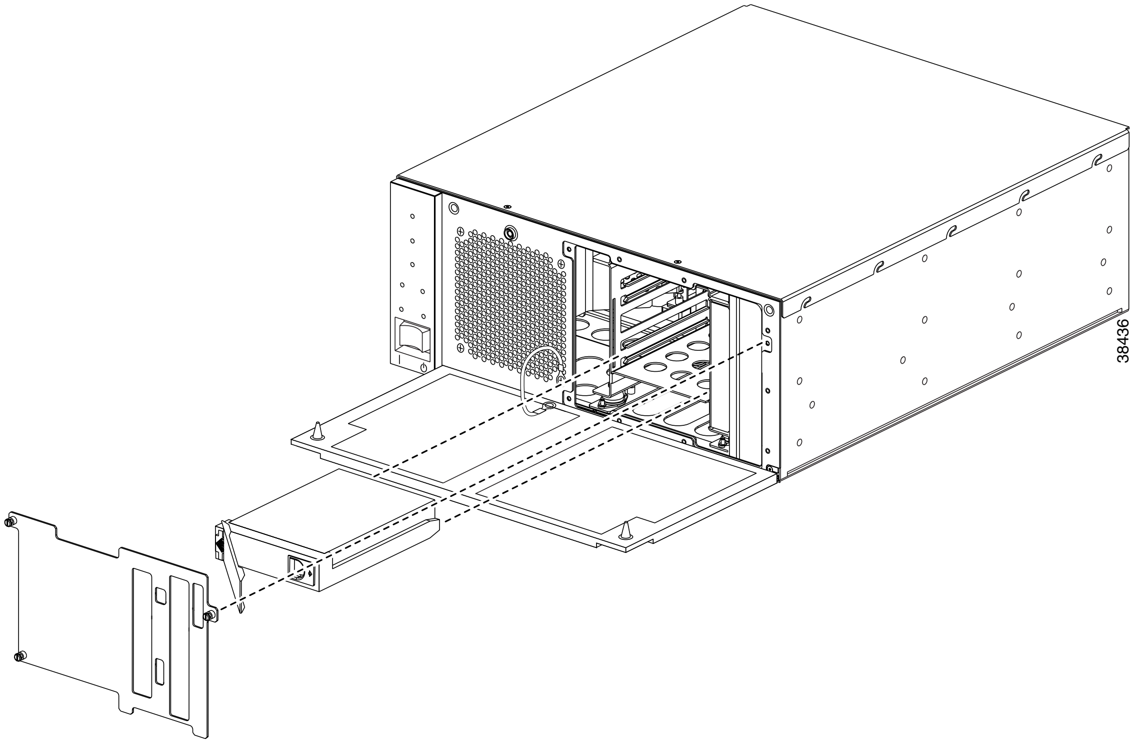
Upgrading Hard Drives

Each of the server platforms require a minimum of two 18-gigabyte hard drives. To upgrade hard drives, follow the procedures in the following sections:

- Removing a Hard Disk Drive, page 5-3
- Installing a Hard Disk Drive, page 5-6

Figure 5-1 provides an example diagram of removing and replacing a hard disk drive from a Netra t 1120/1125 chassis.

Figure 5-1 Removing and Replacing a Hard Disk Drive



Removing a Hard Disk Drive

The procedures for removing a hard disk drive are found in the following sections:

- Removing a Hard Disk Drive from a Netra t 100/105 Chassis, page 5-3
- Removing a Hard Disk Drive from a Netra t 1120/1125 Chassis, page 5-4
- Removing a Hard Disk Drive from a Netra t 1400/1405 Chassis, page 5-5

Caution Use proper ESD grounding techniques when handling components. Wear an antistatic wrist strap and use an ESD-protected mat. Store ESD-sensitive components in antistatic bags before placing them on any surface.

Removing a Hard Disk Drive from a Netra t 100/105 Chassis

Perform the following steps to remove a hard disk drive from a Netra t 100/105 chassis:

Step 1 Shut down the Solaris 2.6 operating system from the console.

Step 2 Turn the power supply switch off.

Step 3 Disconnect the AC power cord (if equipped).

Step 4 Disconnect any other cables.

Step 5 Remove the system from the rack and place at an ESD station.

Step 6 Attach the wrist strap to the attachment point on the station.

Caution Do not touch any metal parts.

Step 7 Remove the front bezel by pressing the latch at either end.

Step 8 Lever the grilles out.

Step 9 Push the handle latch to the right to open the drive handle.

Step 10 Extend the drive handle to disconnect the drive from the system.

Step 11 Holding the drive handle, remove the drive from the drive bay.

Step 12 The hard disk drive rear connector is disconnected when the drive is ejected.

Step 13 Place the drive on an ESD mat.

Removing a Hard Disk Drive from a Netra t 1120/1125 Chassis

Perform the following steps to remove a hard disk drive from a Netra t 1120/1125 chassis:

Step 1 Attach the wrist strap to the chassis.

Caution Wear an antistatic wrist strap and use an ESD-protected mat when handling components. When servicing or removing system unit components, use a wrist strap with a 10 mm press stud connection and attach the wrist strap to the press stud at the front or rear of the chassis. This should be performed before the top cover is removed.

Step 2 Power off the system and remove the input power connectors:

Caution Prior to turning off system power, exit from the operating system. Failure to do so might result in data loss.

a. Momentarily set the front panel ON/STBY system switch to the STBY position until the system powers down.

b. Verify that the Power LED is off.

c. Disconnect the input power connectors on the rear of the unit, or open all circuit breakers associated with the unit.

Caution Regardless of the position of the ON/STBY switch, where a DC power cord remains connected to the system, DC voltage is always present within the power supply. Regardless of the position of the ON/STBY switch, where an AC power cord remains connected to the system, hazardous voltages are always present within the power supply.

Step 3 Open the front access cover.

Step 4 Remove the front ESD screen, using a No.1 Phillips-head screwdriver to undo the two captive screws.

Step 5 Push the handle latch to the right to open the drive handle.

Step 6 Extend the drive handle to disconnect the drive from the system.

Step 7 Holding the drive handle, remove the drive from the drive bay.

Step 8 The hard disk drive rear connector is disconnected when the drive is ejected.

Step 9 Place the drive on an ESD mat.

Removing a Hard Disk Drive from a Netra t 1400/1405 Chassis

Perform the following steps to remove a hard disk drive from a Netra t 1400/1405 chassis:

Step 1 Power off the system and remove the input power connectors:

⚠ **Caution** Prior to turning off system power, exit from the operating system. Failure to do so might result in data loss.

a. Momentarily set the front panel ON/STBY system switch to the STBY position until the system powers down.

b. Verify that the Power LED is off.

c. Disconnect the input power connectors on the rear of the unit, or open all circuit breakers associated with the unit.

⚠ **Caution** Regardless of the position of the ON/STBY switch, where a DC power cord remains connected to the system, DC voltage is always present within the power supply. Regardless of the position of the ON/STBY switch, where an AC power cord remains connected to the system, hazardous voltages are always present within the power supply.

Step 2 Attach the wrist strap to the chassis.

⚠ **Caution** Wear an antistatic wrist strap and use an ESD-protected mat when handling components. When servicing or removing system unit components, use a wrist strap with a 10 mm press stud connection and attach the wrist strap to the press stud at the front or rear of the chassis. This should be performed before the top cover is removed.

Step 3 Remove the lower front cover by turning the six captive quarter-turn Phillips screws to the left, until loose.

Step 4 Push the handle latch to the right to open the drive handle.

Step 5 Extend the drive handle to disconnect the drive from the system.

Step 6 Holding the drive handle, remove the drive from the drive bay.

Step 7 The hard disk drive rear connector is disconnected when the drive is ejected.

Step 8 Place the drive on an ESD mat.

Installing a Hard Disk Drive

The procedures for installing a hard disk drive are found in the following sections:

- Installing a Hard Disk Drive in a Netra t 100/105 Chassis, page 5-6
- Installing a Hard Disk Drive in a Netra t 1120/1125 Chassis, page 5-6
- Installing a Hard Disk Drive in a Netra t 1120/1125 Chassis, page 5-6

Caution Use proper ESD grounding techniques when handling components. Wear an antistatic wrist strap and use an ESD-protected mat. Store ESD-sensitive components in antistatic bags before placing them on any surface.

Installing a Hard Disk Drive in a Netra t 100/105 Chassis

Perform the following steps to install a hard disk drive in a Netra t 100/105 chassis:

Step 1 Ensure the wrist strap is still attached and the system is powered off.

Step 2 Holding the drive handle of the new hard disk drive, insert the drive into the drive bay.

Step 3 Push the front of the drive to connect it to the SCSI bus.

Step 4 Close the drive handle to lock the drive into the system.

Step 5 Replace the grilles and front bezel.

Step 6 Reinstall the system in the rack.

Step 7 Reconnect any cables, including the AC power cord, if equipped.

Step 8 Turn the power supply switch on.

Step 9 Detach the wrist strap.

Step 10 Start up the Solaris 2.6 operating system from the console.

Installing a Hard Disk Drive in a Netra t 1120/1125 Chassis

Perform the following steps to install a hard disk drive in a Netra t 1120/1125 chassis:

Step 1 Ensure the wrist strap is still attached and the system is powered off.

Step 2 Holding the drive handle of the new hard disk drive, insert the drive into the drive bay.

Step 3 Push the front of the drive to connect it to the SCSI bus.

Step 4 Close the drive handle to lock the drive into the system.

Step 5 Replace the front ESD screen using a No.1 Phillips-head screwdriver.

Step 6 Replace the front access cover.

Step 7 Power on the system:

a. Turn on power to all connected peripherals.

Note Peripheral power is activated prior to system power so the system can recognize the peripherals when it is activated.

b. Momentarily set the front panel ON/STBY system switch to the ON position.

Step 8 Detach the wrist strap.

Step 9 Start up the Solaris 2.6 operating system from the console.

Installing a Hard Disk Drive in a Netra t 1400/1405 Chassis

Perform the following steps to install a hard disk drive in a Netra t 1400/1405 chassis:

Step 1 Ensure the wrist strap is still attached and the system is powered off.

Step 2 Holding the drive handle of the new hard disk drive, insert the drive into the drive bay.

Step 3 Push the front of the drive to connect it to the SCSI bus.

Step 4 Close the drive handle to lock the drive into the system.

Step 5 Replace the front cover and secure by turning the six captive quarter-turn screws to the right.

Step 6 Power on the system:

a. Turn on power to all connected peripherals.

Note Peripheral power is activated prior to system power so the system can recognize the peripherals when it is activated.

b. Momentarily set the front panel ON/STBY system switch to the ON position.

Step 7 Detach the wrist strap.

Step 8 Start up the Solaris 2.6 operating system from the console.

Upgrading Processors

Each of the server platforms requires the user of 440 MHz processors. The number of 440 MHz processors required in each server platform is as follows:

- Netra t 100/105—1
- Netra t 1120/1125—2
- Netra t 1400/1405—4

Depending on the number and speed of the processors in your host, you might have to replace your processor or add additional processors. The following sections contain procedures that describe how to remove and replace or add processors:

- Installing 440 MHz Processors, page 5-8
- Removing a CPU Module, page 5-8

- Replacing a CPU Module, page 5-10

Note The CPU in the Netra t 100/105 cannot be upgraded.

Caution You must use processors of identical speed; you cannot mix processors of different speeds.

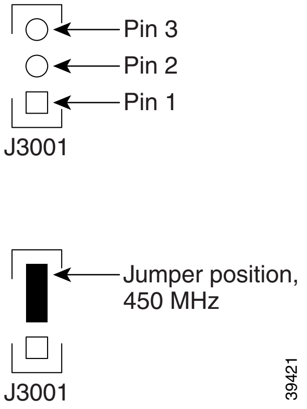
Installing 440 MHz Processors

To install 440 MHz processors, follow the documentation that shipped with your processors. Typically the following documents are included:

- Sun^{TM} 450 MHz UltraSPARC^{TM}-ii Module Upgrade, p/n 806-1055-11
- Sun^{TM} Flash PROM Guide for Workstations and Workgroup Servers—Standalone Version, p/n 802-3233-19

Note If you are using OpenBoot PROM version 3.17.0 or later, you do not need to update the Flash PROM. Set the buffer speed on the motherboard by changing the clocking select jumper J3001 as shown in Figure 5-2.

Figure 5-2 Jumper Position for 450 MHz Processors



Removing a CPU Module

The procedures for removing a CPU module are found in the following sections:

- Removing a CPU Module from a Netra t 1120/1125 Chassis, page 5-9
- Removing a CPU Module from a Netra t 1400/1405 Chassis, page 5-9

Caution Use proper ESD grounding techniques when handling components. Wear an antistatic wrist strap and use an ESD-protected mat. Store ESD-sensitive components in antistatic bags before placing them on any surface.

Removing a CPU Module from a Netra t 1120/1125 Chassis

Perform the following steps to remove a CPU module from a Netra t 1120/1125 chassis:

Step 1 Attach the wrist strap. See instructions in the "Removing a Hard Disk Drive from a Netra t 1120/1125 Chassis" section on page 5-4.

Step 2 Power off the system and remove the input power connectors. See instructions in the "Removing a Hard Disk Drive from a Netra t 1120/1125 Chassis" section on page 5-4.

Step 3 Remove the top access cover:

Caution Wear an antistatic wrist strap and use an ESD-protected mat when handling components. When servicing or removing system unit components, use a wrist strap with a 10 mm press stud connection and attach the wrist strap to the press stud at the front or rear of the chassis. This should be performed before the top cover is removed.

a. Remove the rack fixing screws and withdraw the unit on its slides (if fitted). To remove the top access cover, the unit might need to be completely removed from the rack. If slides are fitted, disconnect the cables and release the slides. Place the system on an approved work station/position.

b. Remove the two screws from the front of the top access cover and carefully store them away from the system unit.

c. Place the system so that the extended tab of the top access cover is facing you. To release the top cover, pull the tab towards you and lift the cover off.

Step 4 After removing the top access cover, using both thumbs, simultaneously lift the two levers on the CPU module upward and to the side.

Step 5 Using the two levers, lift the CPU module upwards until it clears the system chassis.

Step 6 Place the CPU module on an ESD mat.

Removing a CPU Module from a Netra t 1400/1405 Chassis

Perform the following steps to remove a CPU module from a Netra t 1400/1405 chassis:

Step 1 Power off the system and remove the input power connectors. See instructions in the "Removing a Hard Disk Drive from a Netra t 1400/1405 Chassis" section on page 5-5.

Step 2 Attach the wrist strap. See instructions in the "Removing a Hard Disk Drive from a Netra t 1400/1405 Chassis" section on page 5-5.

Step 3 Remove the top access cover:

Caution Wear an antistatic wrist strap and use an ESD-protected mat when handling components. When servicing or removing system unit components, use a wrist strap with a 10 mm press stud connection and attach the wrist strap to the press stud at the front or rear of the chassis. This should be performed before the top cover is removed.

a. Remove the rack fixing screws and withdraw the unit on its slides (if fitted). To remove the top access cover, the unit might need to be completely removed from the rack. If slides are fitted, disconnect the cables and release the slides. Place the system on an approved work station/position.

b. Remove the two screws from the front of the top access cover and carefully store them away from the system unit.

c. Place the system so that the extended tab of the top access cover is facing you. To release the top cover, pull the tab towards you and lift the cover off.

Step 4 After removing the top access cover, using both thumbs, simultaneously lift the two levers on the CPU module upward and to the side.

Step 5 Using the two levers, lift the CPU module upwards until it clears the system chassis.

Step 6 Place the CPU module on an ESD mat.

Replacing a CPU Module

The procedures for replacing a CPU module are found in the following sections:

- Replacing a CPU Module in a Netra t 1120/1125 Chassis, page 5-10
- Replacing a CPU Module in a Netra t 1400/1405 Chassis, page 5-11

Caution Use proper ESD grounding techniques when handling components. Wear an antistatic wrist strap and use an ESD-protected mat. Store ESD-sensitive components in antistatic bags before placing them on any surface.

Replacing a CPU Module in a Netra t 1120/1125 Chassis

Perform the following steps to install a hard disk drive in a Netra t 1120/1125 chassis:

Step 1 Ensure the wrist strap is still attached and the system is powered off.

Step 2 On the antistatic mat, hold the CPU module in an upright position with the plastic surface facing you.

Step 3 Move the levers on the CPU module to point straight upwards.

Step 4 Lower the CPU module along the vertical plastic guides until the module touches the motherboard slot socket. Ensure connectors are aligned. With both hands, simultaneously turn and press the levers downward to the fully horizontal position.

Step 5 Firmly press the module downward into the socket until it is fully seated and the levers are fully locked.

Step 6 Replace the top access cover:

a. Position the top access cover.

b. Push the cover forwards until the lugs on the sides have fully engaged in the slots.

Step 7 Power on the system. See the “Installing a Hard Disk Drive in a Netra t 1120/1125 Chassis” section on page 5-6 for instructions.

Step 8 Detach the wrist strap.

Step 9 Start up the Solaris 2.6 operating system from the console.

Replacing a CPU Module in a Netra t 1400/1405 Chassis

Perform the following steps to install a hard disk drive in a Netra t 1400/1405 chassis:

Step 1 Ensure the wrist strap is still attached and the system is powered off.

Step 2 On the antistatic mat, hold the CPU module in an upright position with the plastic surface facing you.

Step 3 Move the levers on the CPU module to point straight upwards.

Step 4 Lower the CPU module along the vertical plastic guides until the module touches the motherboard slot socket. Ensure connectors are aligned. With both hands, simultaneously turn and press the levers downward to the fully horizontal position.

Step 5 Firmly press the module downward into the socket until it is fully seated and the levers are fully locked.

Step 6 Replace the top access cover:

a. Position the top access cover.

b. Push the cover forwards until the lugs on the sides have fully engaged in the slots.

Step 7 Power on the system. See the "Installing a Hard Disk Drive in a Netra t 1400/1405 Chassis" section on page 5-7 for instructions.

Step 8 Detach the wrist strap.

Step 9 Start up the Solaris 2.6 operating system from the console.

Upgrading Memory

The minimum amount of memory required in each server platform is as follows:

- Netra t 100/105—1 gigabyte
- Netra t 1120/1125—2 gigabytes
- Netra t 1400/1405—4 gigabytes

If you do not have enough memory, you must add additional memory modules of the following types:

- Netra t 100/105—Memory board
- Netra t 1120/1125—Single in-line memory modules (SIMMs)
- Netra t 1400/1405—double in-line memory modules (DIMMs)

The following sections contain procedures that describe how add additional memory:

- Removing a Memory Module, page 5-12
- Replacing a Memory Module, page 5-14

⚠ **Caution** Memory modules consist of electronic components that are extremely sensitive to static electricity. Ordinary amounts of static electricity from clothing or work environment can destroy the memory module.

Caution When removing a SIMM or DIMM, an identical replacement is required. The replacement SIMM or DIMM must be inserted into the same socket as the removed memory module.

Caution Each SIMM or DIMM bank must contain at least two SIMMs or DIMMs of equal density (for example, two 32-megabyte SIMMs) to function properly. Do not mix SIMM or DIMM densities in any bank.

Tip The system unit *must* have at least two identical SIMMs or DIMMs installed in paired sockets of any SIMM or DIMM bank. For best system performance, install four identical SIMMs or DIMMs.

Removing a Memory Module

The procedures for removing memory modules are found in the following sections:

- Removing a Memory Board from a Netra t 100/105 Chassis, page 5-12
- Removing a SIMM from a Netra t 1120/1125 Chassis, page 5-13
- Removing a DIMM from a Netra t 1400/1405 Chassis, page 5-14

Caution Use proper ESD grounding techniques when handling components. Wear an antistatic wrist strap and use an ESD-protected mat. Store ESD-sensitive components in antistatic bags before placing them on any surface.

Removing a Memory Board from a Netra t 100/105 Chassis

Perform the following steps to remove a memory board from a Netra t 100/105 chassis:

Step 1 Power off the system and remove the input power connectors. See the "Removing a Hard Disk Drive from a Netra t 100/105 Chassis" section on page 5-3.

Step 2 Attach the wrist strap. See the "Removing a Hard Disk Drive from a Netra t 100/105 Chassis" section on page 5-3.

Step 3 Remove the cover screw using a Phillips No. 2 screwdriver.

Step 4 Remove the rack brackets, if fitted.

Step 5 Slide the cover to the rear and lift.

Step 6 Lift out the processor cover located in the rear center of the unit. Make sure you slide the processor cover tabs from under the rear I/O card before lifting the processor cover away from the system.

Step 7 Unplug the serial and SCSI cables from the rear I/O board.

Step 8 Using a Phillips No.1 screwdriver, remove the screws and washers from the base memory board.

Step 9 Lift up gently on the memory board to disconnect the three memory board connectors.

Step 10 Place the SIMM on an ESD mat.

Removing a SIMM from a Netra t 1120/1125 Chassis

Perform the following steps to remove a memory board from a Netra t 1120/1125 chassis:

Caution Handle SIMMs only by the edges. Do not touch the SIMM components or metal parts. Always wear a grounding strap when handling a SIMM.

Step 1 Attach the wrist strap. See the "Removing a Hard Disk Drive from a Netra t 1120/1125 Chassis" section on page 5-4.

Step 2 Power off the system and remove the input power connectors. See the "Removing a Hard Disk Drive from a Netra t 1120/1125 Chassis" section on page 5-4.

Step 3 Remove the top access cover. See the "Removing a CPU Module from a Netra t 1120/1125 Chassis" section on page 5-9.

Step 4 Remove the power supply but do not disconnect any restraining power supply cables:

Caution When removing the power supply, attach the copper end of the wrist strap to the system unit chassis, not to the power supply.

a. Using an 8 mm wrench, remove the primary earth connection by removing the M5 nut and captive washer.

b. Using an 8 mm wrench, remove the logic ground connection by removing the two M5 nuts and captive washers.

c. Using a No.2 Phillips-head screwdriver, loosen the eight external and two internal captive screws securing the power supply to the chassis.

d. Using a Phillips No. 2 screwdriver, remove the two captive screws securing the power supply bracket to the chassis front crossmember.

e. Push the power supply forwards slightly to clear the earth grounding stud.

f. Lift the power supply from the chassis until it is restrained by the power supply cables. Rest the power supply on the front crossmember of the enclosure.

g. Remove the cables from the clip retaining them to the processor mounting plate.

h. Disconnect the two cables from the alarms card. (To perform this it might be necessary to remove a PCI card from the chassis.)

i. Disconnect the power supply cables from the motherboard.

j. Disconnect the power supply cable from the removable drive assembly.

k. Disconnect the power supply cable from the hard disk drive assembly or assemblies.

l. Disconnect the power supply cable from the main fan unit.

m. Remove the power supply from the chassis.

Step 5 Rest the power supply on the side of the system enclosure.

Step 6 Locate the SIMM to be removed.

Step 7 Push the lever away from the SIMM to be removed.

Caution Do not use excessive force; the lever can snap.

Step 8 Remove the SIMM from the socket.

Step 9 Place the SIMM on an ESD mat.

Removing a DIMM from a Netra t 1400/1405 Chassis

Perform the following steps to remove a memory board from a Netra t 1400/1405 chassis:

Caution Handle DIMMs only by the edges. Do not touch the DIMM components or metal parts. Always wear a grounding strap when handling a DIMM.

Step 1 Power off the system and remove the input power connectors. See the "Removing a Hard Disk Drive from a Netra t 1400/1405 Chassis" section on page 5-5.

Step 2 Attach the wrist strap. See the "Removing a Hard Disk Drive from a Netra t 1400/1405 Chassis" section on page 5-5.

Step 3 Remove the top access cover. See the "Removing a CPU Module from a Netra t 1400/1405 Chassis" section on page 5-9.

Step 4 Locate the DIMM to be removed.

Step 5 Push the lever away from the DIMM to be removed.

Caution Do not use excessive force; the lever can snap.

Step 6 Remove the DIMM from the socket.

Step 7 Place the DIMM on an ESD mat.

Replacing a Memory Module

The procedures for removing memory modules are found in the following sections:

- Removing a Memory Board from a Netra t 100/105 Chassis, page 5-12
- Removing a SIMM from a Netra t 1120/1125 Chassis, page 5-13
- Removing a DIMM from a Netra t 1400/1405 Chassis, page 5-14

Caution Use proper ESD grounding techniques when handling components. Wear an antistatic wrist strap and use an ESD-protected mat. Store ESD-sensitive components in antistatic bags before placing them on any surface.

Replacing a Memory Board in a Netra t 100/105 Chassis

There is only one installation location for memory in the Netra t 100/105s. There are three sizes of memory available:

- 64 Mbyte memory board (part number 595-5314)

- 256 Mbyte memory board (part number 370-4155)
- 512 Mbyte memory board (part number 595-5316)

Note Do not install memory boards in a stack of three. These boards can only be installed singly or in twos. The 256 Mbyte board is the only board that can be installed in a stack of four.

Perform the following steps to replace a memory board in a Netra t 100/105 chassis:

Step 1 Ensure the wrist strap is still attached and the system is powered off.

Step 2 Position the new spacers over the screw holes.

Step 3 Insert the new, longer screws with their washers through the holes in the new board. Place the spring washer on the screws first, and then the plain washer.

Step 4 Position the secondary memory board above the base memory board so that the connectors line up and the screws pass through the spacers.

Step 5 Engage the screws in their threads to ensure that the board is in the correct position.

Step 6 Press down firmly on all three memory board connectors until they are firmly seated in the connectors on the board beneath. You might find it helpful to seat the middle connector properly before the other two connectors. You will feel a slight click as the connectors engage.

Caution Although it is necessary for the connectors to be properly seated, you must not apply excessive pressure to them. If you do, you might cause micro-fractures on the motherboard which can impair the operation of the board.

Step 7 Tighten the securing screws so that the boards sit firmly on the motherboard.

Step 8 Replace the processor cover located in the rear center of the unit. Make sure you put the tabs of the processor cover back into their original position underneath the rear I/O card.

Step 9 Plug in the serial and SCSI cables to the rear I/O board.

Step 10 Slide the cover forward to close the chassis, and tighten the cover screw using a Phillips No. 2 screwdriver.

Step 11 Replace the rack brackets, if fitted previously.

Step 12 Detach the antistatic wrist strap.

Step 13 Reconnect the input power connectors and power on the system. See the “Installing a Hard Disk Drive in a Netra t 1400/1405 Chassis” section on page 5-7 for instructions.

Replacing a SIMM in a Netra t 1120/1125 Chassis

Table 5-1 identifies SIMM installation locations in the Netra t 1120/1125s.

Table 5-1 SIMM Bank and Bank Quads

Bank	Bank Quad
0	U0701, U0702, U0703, and U0704
1	U0801, U0802, U0803, and U0804

Table 5-1 SIMM Bank and Bank Quads (continued)

Bank	Bank Quad
2	U0901, U0902, U0903, and U0904
3	U1001, U1002, U1003, and U1004

Perform the following steps to replace a SIMM in a Netra t 1120/1125 chassis:

Step 1 Ensure the wrist strap is still attached and the system is powered off.

Step 2 Locate the appropriate SIMM slots on the motherboard.

Note The system unit must have at least two identical SIMMs installed in paired sockets of any SIMM bank. For best system performance, install four identical SIMMs. Table 5-1 identifies SIMM installation locations.

Caution Hold SIMMs only by the edges.

Step 3 Remove the SIMM from the antistatic container.

Step 4 Position the SIMM in the socket, ensuring that the notch is on the same side as the lever.

Step 5 Using your thumbs, press firmly on the top of the SIMM until it is properly seated.

Caution Do not use excessive force; the lever can snap. Apply even, lateral pressure to the lever when seating the SIMM. Make sure the SIMM is level when pushing it into the socket.

Note Proper SIMM seating is verified by a clicking sound. Ensure the SIMM is properly seated.

Step 6 Replace the power supply:

a. Position the power supply above the chassis. Rest it, upside-down (unlabeled side up), on the front crossmember of the enclosure.

b. Connect the power cable to the removable media drive assembly (if fitted).

c. Connect the three main power supply cables to the motherboard.

d. Connect the power cable to the SCSI backplane assembly.

e. Connect the power cable to the main fan assembly.

f. Connect the cable connector to the alarms card.

g. Position the power supply toward the rear of the chassis until the power supply rear panel is flush with the chassis.

h. Using a No.2 Phillips-head screwdriver, tighten the eight captive screws securing the power supply to the rear of the chassis.

i. Using a No.2 Phillips-head screwdriver, tighten the two captive screws securing the power supply bracket to the chassis front crossmember.

j. Using a No.2 Phillips-head screwdriver, tighten the captive screw within the PSU to the chassis L-bracket.

k. Using an 8 mm wrench, secure the primary earth connection by tightening the M5 nut and captive washer.

l. Using an 8 mm wrench, secure the logic ground connection by tightening the two M5 nuts and captive washers.

m. Replace the top access cover.

Step 7 Detach the wrist strap.

Step 8 Replace the top access cover. See the "Replacing a CPU Module" section on page 5-10.

Step 9 Reconnect the input power connectors and power on the system. See the "Installing a Hard Disk Drive" section on page 5-6 for instructions.

Replacing a DIMM in a Netra t 1400/1405 Chassis

Table 5-2 identifies DIMM installation locations in the Netra t 1400/1405s.

Table 5-2 DIMM Bank and Bank Quads

Bank	U Number (Motherboard)	U Number (Memory Riser Card)
0	U1301 and U1302	U0301 and U0302
2	U1303 and U1304	U0303 and U0304
1	U1401 and U1402	U0401 and U0402
3	U1403 and U1404	U0403 and U0404

Perform the following steps to replace a DIMM in a Netra t 1400/1405 chassis:

Step 1 Ensure the wrist strap is still attached and the system is powered off.

Step 2 Locate the appropriate DIMM slots on the motherboard.

Note The system unit must have at least two identical DIMMs installed in paired sockets of any DIMM bank. For best system performance, install four identical DIMMs. Table 5-2 identifies DIMM installation locations.

Caution Hold DIMMs only by the edges.

Step 3 Remove the DIMM from the antistatic container.

Step 4 Position the DIMM in the socket, ensuring that the notch is on the same side as the lever.

Step 5 Using your thumbs, press firmly on the top of the DIMM until it is properly seated.

Note Proper DIMM seating is verified by a clicking sound. Ensure the DIMM is properly seated.

Step 6 Replace the top access cover. See the "Removing a CPU Module from a Netra t 1400/1405 Chassis" section on page 5-9.

Step 7 Detach the antistatic wrist strap.

Step 8 Reconnect the input power connectors and power on the system. See the "Installing a Hard Disk Drive in a Netra t 1400/1405 Chassis" section on page 5-7 for instructions.

Verifying The Hardware Installation

After installing new hardware components, you can run a diagnostic program to ensure the system recognizes your components.

To run the diagnostic program:

Step 1 Start at the ok prompt and enter:

```
setenv auto-boot? false
setenv diag-switch? true
```

This disables automatic booting and runs a diagnostic program.

Step 2 Unplug the network Ethernet cable from the machine.

Details about the system components, including hard drives, memory, and processors, appear on the screen. If you do not see the components you recently installed, you must perform troubleshooting steps to determine the problem. Contact the Cisco TAC for assistance in troubleshooting. See the "Obtaining Technical Assistance" section on page xviii for more information.

Step 3 The machine eventually stops trying to boot from the network and returns to the ok prompt. Enter the following commands:

```
setenv auto-boot? true
setenv diag-switch? false
```

Step 4 Reboot the machine.

Where to Go Next

This completes upgrading your hardware. Return to the appropriate upgrade procedure for your solution for the next step in your upgrade.

CHAPTER 6

Installing the Operating System on the SC Hosts

This chapter describes installation of the Sun Solaris 2.6 operating system, Solaris patches, alarm card software, and Volume Manager software on the SC host.

Note This chapter is provided only for upgrades from the Cisco DAS Release 2.0 to the Cisco SS7 Interconnect for Access Servers Solution Release 2.x. Other solution upgrades do not require that the steps in this chapter be performed.

Note The Cisco SC software must be run on the Sun Solaris 2.6 operating system. Other versions of the Sun Solaris operating system are not supported.

This chapter contains the following sections:

- Before You Start, page 6-2
- Connecting to the SC Host, page 6-3
- Stopping the SC Software, page 6-3
- Installing the Sun Solaris 2.6 Operating System, page 6-4
- Installing the Sun Solaris Patches, page 6-15
- Installing the Alarm Card Software, page 6-17
- Installing the Volume Manager, page 6-22

Note The procedures in this chapter assume that the system is powered on, with both boot disks (A-DSK0 and B-DSK0) removed and booted to the `{0} ok` prompt. To power on a CPU, push both tabs outward (away from the center). When you are instructed to power off a CPU in the procedures that follow, pull both tabs on the CPU toward the center.

Tip You can automate Sun Solaris installations by using JumpStart automated installation technology (not described in this document). Refer to the Sun web site for more information. Cisco recommends this resource: Automating Solaris^{TM} Installations: A Custom JumpStart Guide, by Paul Anthony Kasper and Alan L. McClellan. First edition; 320 pages, ISBN 0-13-312505-X.

Before You Start

Note The procedures in this chapter require a working knowledge of the system administration procedures for the Sun Solaris (UNIX) operating system.

- Obtain the following information specific to your target Sun Netra machine from your system site administrator:
  - Host name of target machine
  - IP address of target machine
  - Root password
  - Default router IP address
  - Second Ethernet IP address
- Allow at least two hours downtime to install the Sun 2.6 operating system.

Caution In a simplex configuration, call processing will stop now. The host will not be able to process calls until you restart the software after the upgrade. See the "Restarting the SC Software" section on page 7-56. In a high-availability configuration, perform these steps on the standby host first. Unless the active host goes down, call processing will not stop.

- Obtain the following CD-ROM disks:
  - Sun Solaris^{TM} Operating Environment Installation CD, September 1999, p/n: 704-6914-10
  - Sun Solaris^{TM} 2.6 Software, p/n: 704-6220-10
  - Sun Solaris^{TM} 2.5.1 Software, to be used if you need to back out of the Sun Solaris 2.6 upgrade and reinstall Sun Solaris.
  - Netra t 11xx alarm card software CD, p/n 704-6330-10
  - Cisco Telephony Controller Software Release 7.3(x) CD or Cisco Media Gateway Controller Release 7.4(x) CD

Note If your processors are less than 419 MHz and you do not use the Operating Environment Installation CD to install the Sun 2.6 operating system, the interactive installation screen display differs from the two-CD installation process documented in this guide; however, the final result is the same.

- You will need the following additional installation files:
  - Sun Solaris^{TM} 2.6 patch software (CSCOh007.pkg)
  - Cisco Installation package (CSCOh005.pkg) for log and spool file installation.
- You may need to obtain the following optional components, depending upon the system options you are installing:
  - Sun StorEdge Volume Manager 2.6, p/n: 704-6316-10
  - Cisco Installation package (CSCOh006.pkg) for Volume Manager 2.6 software
  - Netra t 11xx alarm card software CD, p/n 704-6330-10, if installing alarm card software.

- The target machine must have a terminal connected by using a serial cable inserted into the console port.
- Target machines from CTDI come with the Volume Manager License key. However, if your target machine source is not CTDI, you must obtain the Volume Manager License key from Sun Microsystems. Follow the instructions on the software license key request form to obtain a Volume Manager License key.
- Have your company's internal support and Cisco support contact information readily available so you can get help with the installation if needed. If you have questions or need assistance, see the "Obtaining Technical Assistance" section on page xviii.

Tip Monitor system output frequently for error messages during the installation process and correct any error conditions before continuing with the installation.

Connecting to the SC Host

Connect your laptop processor's COM port to Port A on the SC host, and open a console connection using a terminal emulation program (such as Reflection). Cisco recommends selecting DEC VT100 as the terminal type. The PC Console terminal type does not work very well.

Note For procedures in this document, you must log into the system as the root user. Do not log in as another user and enter **su** to become root.

Your software should have been stopped if you backed up your data per the instructions in Chapter 2, "Backing Up Your SC Host Data." To verify that the software is stopped, proceed to the "Stopping the SC Software" section on page 6-3.

Stopping the SC Software

Step 1 To check if the SC software is running, enter **ps -ef | grep procM**:

```
va-cerulean% ps -ef | grep tran
```

Step 2 If you receive a response showing the system is running, shut down the SC software by entering the **/etc/init.d/transpath** stop command:

```
va-lions:8> /etc/init.d/transpath stop
Signalling procM to shut down
...shutdown complete
```

Caution This stops all processing of calls if you are logged in to the active server.

Step 3 Verify that the system has stopped by again entering the following:

```
ps –ef | grep procM
```

Make sure that you receive no response.

Installing the Sun Solaris 2.6 Operating System

This section provides instructions for installing the operating system on the Sun Netra t 1120, t 1125, and E450 platforms. There are points in the instructions when the responses you make to prompts depend on the disk drive size or other particulars of your system. These places are pointed out as you go.

This section contains the following procedures:

- Booting from a Local CD-ROM, page 6-4
- Loading the Sun Solaris 2.6 Operating System, page 6-8
- Installing the Sun Solaris Patches, page 6-15
- Installing the Alarm Card Software, page 6-17
- Configuring a Second Ethernet Interface, page 6-21
- Configuring a Second Disk Drive, page 6-21

Booting from a Local CD-ROM

To boot from a local CD-ROM, perform the following steps:

Step 1 Put the “Operating Environment Installation CD,” part number 704-6914-10, into the CD-ROM drive.

Caution **For Sun Netra t 112x**: Leave the front CD panel open during the installation of CD-ROM-based software on a Sun Netra t 112x machine. Some installation routines automatically eject the CD when finished. If the front panel is closed, damage can occur when the CD is ejected.

Note Due to a known Sun bug, some installation routines may not automatically eject the CD when installing the Sun Solaris 2.6 operating system before the installation of the Cisco patch packages. You must copy patch 107665-01.tar.Z to a local directory. This patch will re-enable the CD-ROM.

Step 2 If the system is currently running, log in as root and shut it down:

```
# init 0
```

Step 3 From the `ok` prompt, boot the CD-ROM:

```
{0} ok boot cdrom
```

Note This process may take approximately 5 minutes to run.

If the machine has never had an operating system installed, the following screen appears when the CD-ROM boot is finished:

```
Boot device: /pci@1f,4000/scsi@3/disk@6,0:f  File and args:
SunOS Release 5.7 Version Generic_106541-06 [UNIX(R) System V Release 4.0]
Copyright (c) 1983-1999, Sun Microsystems, Inc.
Solaris Web Start 3.0 installer
No frame buffer found.
```

```
Command line install is available in english only.

English has been selected as the language in which to perform the install.
Starting the Web Start 3.0 Solaris installer

Solaris installer is searching the system's hard disks for a
location to place the Solaris installer software.

The default root disk is /dev/dsk/c0t0d0.
The Solaris installer needs to format
/dev/dsk/c0t0d0 to install Solaris.

WARNING: ALL INFORMATION ON THE DISK WILL BE ERASED!

Do you want to format /dev/dsk/c0t0d0?  [y,n,?,q]
```

If an operating system was previously installed on the machine, text similar to the following appears with two warnings:

```
Command line install is available in english only.

English has been selected as the language in which to perform the install.
Starting the Web Start 3.0 Solaris installer

Solaris installer is searching the system's hard disks for a
location to place the Solaris installer software.

This system appears to contain a version of Solaris.
The Solaris installer does not allow upgrading. If you
choose to use this installer an initial install will be
required. Any information on your system's disks could be erased.

Would you like to use this installer?   [y,n,?]
```

Step 4 In all of the above cases, type **y** and press **Enter** to continue until the following text appears:

```
Enter a swap partition size between 320Mb and 17269Mb, default = 512Mb [?]
```

Step 5 Type in **2040** (for 9- and 18-GB disk drives) for swap partition size and press **Enter.** It is not necessary to enter “Mb” after the number; the system assumes that the entry is in megabytes.

```
You have selected /dev/dsk/c0t0d0 with a swap size of 2040/320 to be used by the Solaris
installer.
WARNING: ALL INFORMATION ON THE DISK WILL BE ERASED!
Is this OK  [y,n,?,q]
```

Step 6 Begin the installation by typing **y** and pressing **Enter**. The system copies the necessary files from the CD-ROM and reboots.

Tips This process takes approximately 10 minutes to run and requires no user intervention.

The following text appears:

```
Welcome to the Web Start Solaris Command Line installation!
The following questions will gather information about this system.
This information will be used to configure:

        Network
        Name Service
        Date and Time
        Root Password
        Power Management

     <Press Return to continue>
```

Step 7 Press **Enter** to continue. The following text appears:

```
Please enter a host name, which identifies this system on the network.  The name must be
unique within the domain in which it resides; creating a duplicate host name will cause
problems on the network after you install Solaris.

A host name must be at least two characters; it can contain letters, digits, and minus
signs (-).

Enter host name: <host-name>
```

Step 8 Type the host name of the target Sun Netra machine and press **Enter.**

Note The host name must be unique for each host.

The following text appears:

```
Please specify whether your system will be networked.  Specify Yes if the
system is connected to the network by one of the Solaris or vendor
network/communication Ethernet cards that are supported on the Solaris CD. See
your hardware documentation for the current list of supported cards.

Specify No if the system is connected to a network/communication card that is
not supported or not connected to a network.

Is this machine networked (y/n) [n]?
```

Step 9 Type **y** and press **Enter** to specify that this machine is networked. The following text appears:

```
Please enter the Internet Protocol (IP) Address for this system.  It must be unique and
follow your site's address conventions, or a system/network failure could result.

IP Addresses contain four sets of numbers separated by periods (for example 129.200.9.1).

Enter this machine's IP Address:
```

Step 10 Type the IP address assigned to this system in dotted decimal format and press **Enter**. The following text appears:

```
Please specify the netmask of your subnet.  A default netmask is shown; do not accept the
default unless you are sure it is correct for your subnet. A netmask must contain four
sets of numbers separated by periods (for example 255.255.255.0).
Enter the subnet netmask [255.255.255.0]:
```

Step 11 Type the IP netmask for the subnet and press **Enter**.

Caution Do not accept the default netmask unless you are sure it is correct for your subnet.

The following text appears:

```
Please provide name service information.  Select the name service that will be used by
this system, or None if your system will either, not use a name service at all, or if it
will use a name service not listed here

Available name services:
```

```
1. NIS+
2. NIS
3. DNS
4. None

Please enter the number corresponding to the type of name service you
would like [ ]:
```

Step 12 Type **4** for None and press **Enter.** You can specify a default time zone in one of three ways, described by the text that appears:

```
Please select how to specify your default time zone.

Specify Time Zone by:

1. Geographic region
2. Offset from GMT
3. Time zone file

Please enter the number corresponding to how you would like to specify
the time zone [1]:
```

Step 13 Type the means of defining your default time zone (1, 2, or 3) and press **Enter**. The text that follows prompts you for appropriate input until the following message appears:

```
The default date and time is (current date and time of defined time zone). Do you
want to use this date and time (y/n) [y]?
```

Step 14 Press **Enter** to accept the date and time information as shown, or type **n** and press **Enter** to be prompted for different values. When the information is correct, press **Enter** again. The following text appears:

```
Type in an alphanumeric string to be used as the root password for the computer you are
setting up.
Enter the root password []:
```

Step 15 Type a root password and press **Enter**: The following text appears, prompting you to confirm the root password that you assigned:

```
Retype the above password for confirmation.

Enter the root password again []:
```

Step 16 Retype the root password and press **Enter**. The following text appears:

```
Do you want Power Management turned on (y/n) [n]?
```

Step 17 Disable Power Management by typing **n** and pressing **Enter**. The following text appears:

```
You can choose to be asked the preceding question every time you reboot the system.
Alternatively, you can choose never to be asked about Power Management again.

Ask about Power Management at each reboot (y/n) [n]?
```

Step 18 Type **n** and press **Enter**. The following text appears:

```
You have entered the following values:

Host Name:                 host-name
IP Address:                IP_address
System part of a subnet:   Yes
Netmask:                   IP_netmask
Name Service:              NONE
Time Zone:                 time_zone
Power Management:
                            Turn Power Management Off
                            Do not ask about Power Management at reboot.

Enter 'y' to apply these values and proceed to the next stage of the
installation, or 'n' to return to the beginning and make changes (y/n):
```

Step 19 Make sure that your values are correct before continuing:

a. If your values are incorrect, type **n** and press **Enter** to go back to Step 7.

b. If your values are correct, type **y** and press **Enter** to continue to the installation of the Sun Solaris operating system.

This completes the process of booting from a local CD. Continue with the “Loading the Sun Solaris 2.6 Operating System” section on page 6-8.

Loading the Sun Solaris 2.6 Operating System

This section provides the procedure for loading the Sun Solaris 2.6 operating system.

Note This procedure covers 9- and 18-GB disk drives.

Step 1 Upon acceptance of Step 19 above, the following text appears:

```
keyserv: failed to generate host's netname when establishing root's key.

Solaris Web Start will now gather information to install software for Solaris.

Please wait while initial values are loaded...

Available operating environments:

1.   Solaris 2.5.1 Hardware: 11/97
2.   Solaris 2.6 5/98

Select the number corresponding to the operating environment you would like to install
[1]:
```

Step 2 Type **2**, then press **Enter**. The following text prompts you to verify your choice:

```
You have selected:

Solaris OS:   Solaris 2…6
Enter 'y' if this is correct, or 'n' if it is incorrect:
```

Step 3 When the display shows the software that you have chosen, type **y** and press **Enter** to accept. The following text appears:

```
Please insert the Solaris 2.6 CD.
   <Press Return after the CD has been inserted>
```

Step 4 The Operating Environment Installation CD automatically ejects from the machine at this time. Remove it from the CD-ROM drive and insert the Sun Solaris 2.6 Operating System CD, then press **Enter**. The following screen appears:

```
Reading CD for Solaris 2.6
Please wait while the system is initializing...
```

```
To install basic Solaris products into their default directory locations, select Default
Install.

Custom install provides a choice of which Solaris products to install.  For each product,
it also provides an option to further customize the products install.

Types of install available:

1. Default Install
2. Custom Install

Select the number corresponding to the type of install you would like [1]:
```

Step 5 Type **2** for Custom Install, and press **Enter**. The following text appears:

```
Select the software localizations you want to install. The English version of Solaris will
be installed by default.

Enable locale German ( de ) (y/n) [n]?
```

Step 6 Type **n** and press **Enter.** The following text appears:

```
Enable locale Spanish ( es ) (y/n) [n]?
```

Step 7 Type **n** and press **Enter.** The following text appears:

```
Enable locale French ( fr ) (y/n) [n]?
```

Step 8 Type **n** and press **Enter.** The following text appears:

```
Enable locale Italian ( it ) (y/n) [n]?
```

Step 9 Type **n** and press **Enter.** The following text appears:

```
Enable locale Swedish ( sv ) (y/n) [n]?
```

Step 10 Type **n** and press **Enter** to continue. The following text appears:

```
Available locales:

1. English (Australia) ( en_AU )
2. English (Canada) ( en_CA )
3. English (Ireland) ( en_IE )
4. English (New Zealand) ( en_NZ )
5. English (UK) ( en_UK )
6. English (United States) ( en_US )
7. English (POSIX C) ( C )

Select the number corresponding to the desired system locale [6]:
```

Step 11 Type the number corresponding to the appropriate locale and press **Enter**. The following text appears:

```
Available software groups:

1.   Entire Solaris Software Group Plus OEM
2.   Entire Solaris Software Group
3.   Developer Solaris Software Group
4.   End User Solaris Software Group
5.   Core Solaris Software Group

Select the number corresponding to the desired Solaris software group [2]:
```

Step 12 Type **1** for “Entire Solaris Software Group Plus OEM” and press **Enter**. The following text appears:

```
Please wait while the system is initializing...
```

```
Select which disks you want to lay out the file systems on.
Required disk space: 2,705 MB
```

One of the following tables appears, depending on your disk size:

```
---------------------------------------------
    9 Gbyte disk drive

Available Disks
   Disk      Size
 c0t0d0    8633 MB
 c0t1d0    8633 MB

---------------------------------------------

18 Gbyte disk drive

Available Disks:
   Disk      Size
 c0t0d0    17269 MB
 c0t1d0    17269 MB

---------------------------------------------
```

Tips Take note of the disk drive size on the target machine. You will need this number when asked to define the disk partitions in a later step.

You also see the following prompt:

```
Enter 'y' to layout file systems on the specified disk.  This will erase all existing data
on the disk.  Enter 'n' to leave the disk unmodified.

Layout file systems on disk c0t0d0 (bootdisk) (y/n) [y]?
```

Step 13 Type **y** and press **Enter** to continue. The following text appears:

```
Layout file systems on disk c0t1d0 (y/n) [n]?
```

Step 14 Type **n** and press **Enter** to continue. The following text appears:

```
File System operations:

1. Print the current partition table
2. Modify a disk's partition table
3. Done

Select the number corresponding to a file system operation, or 'Done' to
proceed with the install [3]:
```

Step 15 Type **2** and press **Enter** to set up the disk partitions. One of the following tables appears:

```
---------------------------------------------
9 Gbyte disk drive

Available disks:

1.  c0t0d0
       /             668 MB
       swap         2040 MB
       /export/home 14561 MB

2.  c0t1d0  Not Selected
```

```
3. Done

---------------------------------------------

9 Gbyte disk drive

Available disks:

1.  c0t0d0
        /             667 MB
       swap          2040 MB
       /export/home  5926 MB

2.  c0t1d0  Not Selected

3. Done

---------------------------------------------
```

You also see the following prompt:

```
Select a disk to modify, or Done to return to the previous menu [3]:
```

Step 16 Type **1** to modify the partitions on disk c0t0d0 and press **Enter**. One of the following tables appears:

```
---------------------------------------------
18 Gbyte disk drive

Disk Name      c0t0d0
 TotalSpace     17269
 Used Space     17269
 Free Space     0
 Round Error    0

 #   Slice Name    Slice Size  Minimum Size
 0.  /             668 MB      665 MB
 1.  swap          2040 MB     2040 MB
 3.  Unused
 4.  Unused
 5.  Unused
 6.  Unused
 7.  /export/home  14561 MB    0 MB

 8.  Done

---------------------------------------------

9 Gbyte disk drive

Disk Name      c0t0d0
 TotalSpace     8633
 Used Space     8633
 Free Space     0
 Round Error    0

 #   Slice Name    Slice Size  Minimum Size
 0.  /             667 MB      665 MB
 1.  swap          2040 MB     2040 MB
 3.  Unused
 4.  Unused
 5.  Unused
 6.  Unused
 7.  /export/home  5926 MB     0 MB
 8.  Done
---------------------------------------------
```

Step 17 You also see the following prompt:

```
Select a slice to modify, or Done to return to the previous menu [8]:
```

Step 18 Remove partition 7 by typing **7** and pressing **Enter**. The following text appears:

```
Enter new slice name:
```

Step 19 Remove the name associated with partition 7 by pressing **Enter**. The screen shows that partition 7 is "Unused."

Step 20 Repeat Step 16 through Step 19 for each partition numbered 4 through 6. Use the screen display example in Step 23 for partition names and sizes.

Note You defined partition 1 (swap) in Step 5 of the section "Booting from a Local CD-ROM".

Step 21 Type the number of the partition to be defined and press **Enter**. The following text appears:

```
Enter new slice name:
```

Step 22 Type the partition name and press **Enter**. The following text appears:

```
Enter new slice size (in MB) [default]:
```

Note When defining the partition size, you need not enter "MB" after the number. The system assumes that the entry is in megabytes.

Step 23 Type the partition size and press **Enter**. Each time a partition is defined, the changes are displayed on the screen. The tables below show the end result of defining the drive partitions for each drive size:

```
---------------------------------------------

18 Gbyte disk drive

Disk Name      c0t0d0
 TotalSpace     17269
 Used Space     17208
 Free Space     61
 Round Error    0

 # Slice Name Slice Size Minimum Size
 0.  /          668 MB      619 MB
 1.  swap       2040 MB     2040 MB
 3.  Unused
 4.  /opt       11040 MB    25 MB
 5.  /var       1025 MB     22 MB
 6.  /usr       2435 MB     0 MB
 7.  Unused

 8.  Done

---------------------------------------------

9 Gbyte disk drive

Disk Name      c0t0d0
 TotalSpace     8633
 Used Space     8627
 Free Space     15
 Round Error    0

 # Slice Name  Slice Size  Minimum Size
 0.  /           512 MB      42 MB
 1.  swap        2040 MB     2040 MB
 3.  overlap     86330 MB
 4.  /opt        4530 MB     25 MB
 5.  /var        1025 MB     22 MB
 6.  /usr        512 MB     578 MB
 7.  Unused
 8.  Done

---------------------------------------------

Select a slice to modify, or Done to return to the previous menu:
```

Step 24 To end disk partitioning, type **8** (for 9- and 18-GB disk drives) and press **Enter**. One of the following tables appears:

```
---------------------------------------------

9 Gbyte disk drive

Available disks:

1.  c0t0d0
         /     512 MB
         swap  2048 MB
      overlap  8633 MB
         /opt  4530 MB
         /var  1025 MB
         /usr  512 MB

2.  c0t1d0  Not Selected

3. Done

---------------------------------------------

18 Gbyte disk drive

Available disks:

1.  c0t0d0
         /     668 MB
         swap  2040 MB
         /opt  11040 MB
         /var  1025 MB
         /usr  2435 MB

2.  c0t1d0  Not Selected

3. Done

---------------------------------------------

Select a disk to modify, or Done to return to the previous menu [3]:
```

Step 25 Type **3** and press **Enter** to continue. The following text appears:

```
File System operations:
```

```
1. Print the current partition table
2. Modify a disk's partition table
3. Done

Select the number corresponding to a file system operation, or 'Done' to
proceed with the install [3]:
```

Step 26 Type **3** and press **Enter** to continue. The following text appears:

```
The following items will be installed:

 Solaris OS:              Solaris 2.6
 Software Locales:        none
 System Locale:           English (United States) ( en_US )
 Solaris Software Group:  Entire Solaris Software Group Plus OEM

   Enter 'y' to accept these values and start the installation, or 'n' to
   return to the beginning and make changes (y/n):
```

Step 27 Type **y**, then press **Enter** to continue.

The process takes approximately 30 minutes to run and does not require user intervention. The following screen gradually appears:

```
Installing...

Installing Solaris software group
|-1%------------25%----------------50%----------------75%-------------100%|
Installing Additional Software
|-1%------------25%----------------50%----------------75%-------------100%|

Installation details:

     Product              Result     More Info
1.    Solaris 2.6 5/98   Installed  Available
2.  Additional Software  Installed  Available
3.  Done

   Enter the number corresponding to the desired selection for more
   information, or Done to continue [3]:
```

Step 28 Type **3** and press **Enter** to continue. The following screen appears:

```
The system needs to reboot to complete installation.

<Press Return to reboot>
```

Step 29 Press **Enter** to reboot the system.

Step 30 The Sun Solaris Software CD is automatically ejected from the CD-ROM drive. Remove the CD.

Step 31 If you wish to define the default gateway after the system has rebooted, log in as root, type the following command, and press **Enter**:

```
# route add default default router IP address 1
```

Note The *default router IP address* is usually **1** (first gateway), but can be any valid number representing any available gateway.

Step 32 To make the default gateway permanent, create a file called /etc/defaultrouter and put the default gateway IP address on the first and only line of the file by entering the following command:

```
# echo default gateway IP address > /etc/defaultrouter
```

Step 33 Verify that the correct Network Time Protocol (NTP) packages are installed by entering the following command:

```
pkginfo | grep ntp
```

The following text displays:

```
system      SUNWntpr       NTP, (Root)
system      SUNWntpu       NTP, (Usr)
```

Note NTP synchronizes call detail record (CDR) timestamps on SC2200s and BAMS. Make sure that the correct NTP packages are installed.

Step 34 Echo the NTP server IP Address into the file /etc/inet/ntp.conf by entering the following command (the NTP server address is provided by your system administrator):

```
# echo "server <NTP server address>" > /etc/inet/ntp.conf
```

Step 35 Enter the following command to re-start the machine:

```
# init 6
```

Step 36 Log in as root.

Step 37 Verify that the daemon **xntpd** is running by entering the following command:

```
ps -ef | grep ntp
```

The following text displays:

```
root    224     1  0 13:59:25 ?        0:00 /usr/lib/inet/xntpd
siggen   424   415  0 14:15:28 pts/1    0:00 grep ntp
vao-siggen-1%
```

This completes the installation of the Sun Solaris 2.6 operating system. Proceed to the “Installing the Sun Solaris Patches” section on page 6-15. If you have questions or need assistance, see the “Obtaining Technical Assistance” section on page xviii.

Installing the Sun Solaris Patches

In this section, the patch cluster is installed on the target machine.

To install the Sun Solaris 2.6 patches, perform the following steps:

Step 1 Insert the CD containing the Sun Solaris 2.6 patches for the Cisco MGC software into the CD-ROM drive.

Step 2 Install the Sun Solaris 2.6 software patches by entering the following commands:

```
# pkgadd -d cdrom/cdrom0/solaris_patches/CSCOh007.pkg
```

The following screen appears:

```
The following packages are available:
  1  CSCOh007     Media Gateway Controller Solaris 2.6 patch cluster

Select package(s) you wish to process (or 'all' to process
all packages). (default: all) [?,??,q]:
```

Step 3 Press **Enter** to accept the default response of **all** and continue. The following screen appears:

```
Processing package instance <CSCOh007> from </cdrom/ciscomgc_install/CSCOh007.pkg>

Media Gateway Controller Solaris 2.6 patch cluster
(sparc) 1.0(1)
Cisco System, Inc.

The selected base directory </opt/sun_install> must exist before
installation is attempted.

Do you want this directory created now [y,n,?,q]
```

Step 4 Type **y** and press **Enter** to continue. The following text appears:

```
Using </opt/sun_install> as the package base directory.
## Processing package information.
## Processing system information.
   1 package pathname is already properly installed.
## Verifying disk space requirements.
## Checking for conflicts with packages already installed.

The following files are already installed on the system and are being
used by another package:
* /opt/sun_install <attribute change only>

* - conflict with a file which does not belong to any package.

Do you want to install these conflicting files [y,n,?,q]
```

Step 5 Type **y** and press **Enter** to continue. The following text appears:

```
## Checking for setuid/setgid programs.

This package contains scripts which will be executed with super-user
permission during the process of installing this package.

Do you want to continue with the installation of <CSCOh007> [y,n,?]
```

Step 6 Type **y** and press **Enter** to continue. The following text appears:

```
Installing Media Gateway Controller Solaris 2.6 patch cluster as <CSCOh007>

## Executing preinstall script.
Platform is SUNW,Ultra-60

NOTICE: Architecture checks passed

## Installing part 1 of 1.
/opt/sun_install/checkPackages2.6
/opt/sun_install/checkPatches2.6
/opt/sun_install/installPatches2.6
/opt/sun_install/packages2.6
/opt/sun_install/patch_optional2.6
/opt/sun_install/patch_order2.6
/opt/sun_install/patch_required2.6
/var/tmp/105181-19.tar.Z
/var/tmp/105210-27.tar.Z
.
.
/var/tmp/108199-01.tar.Z
/var/tmp/108201-01.tar.Z
[ verifying class <none> ]
## Executing postinstall script.
```

```
!!
!!  You must now change directories to /opt/sun_install and
!!  run the installPatches2.6 script as root.
!!


Installation of <CSCOh007> was successful.
```

Step 7 Complete the installation of the Sun Solaris 2.6 software patches by typing the following command then press **Enter**:

```
# cd /opt/sun_install
```

Step 8 Continue to complete the installation of the Sun Solaris 2.6 software patches by typing the following command then press **Enter**

```
# ./installPatches2.6
```

Note This may take about 20 minutes.

The following screen appears:

```
*** InstallPatches2.6 begins Thu Mar 16 10:49:01 GMT 2000 ***

Platform is SUNW,Ultra-60
Changed to /var/tmp directory
Uncompressing 106125-08 ...
Extracting 106125-08 ...
Extraction of patch 106125-08 successful
Installing 106125-08 ...
.
.
Uncompressing 105591-07 ...
Extracting 105591-07 ...
Extraction of patch 105591-07 successful
Installing 105591-07 ...
*** InstallPatches2.6 ends Thu Mar 16 11:07:38 GMT 2000 ***
```

This completes the installation of the Sun Solaris patches. If you have questions or need assistance, see the “Obtaining Technical Assistance” section on page xviii.

If you need alarm card software, continue to the “Installing the Alarm Card Software” section on page 6-17. If you do not need alarm card software, continue to the “Configuring a Second Ethernet Interface” section on page 21.

Installing the Alarm Card Software

To install the alarm card software for the Sun Netra t 112x, perform the following steps:

Step 1 Insert the Sun Netra t 11xx CD into the CD-ROM drive.

Step 2 Start the installation by typing each of the following commands at a # prompt and pressing **Enter**:

```
# cd /cdrom/netrat_11xx_1_0
# pkgadd -d .
```

```
The following packages are available:
  1  SUNWtsalm     TS91 Alarm and Monitor Manpages
                   (sparc.sun4u) 1.0,REV=1.1
  2  SUNWtsalr     TS91 Alarm and Monitor driver
                   (sparc.sun4u) 1.0,REV=1.1
  3  SUNWtsalu     TS91 Alarm and Monitor Utilities
                   (sparc.sun4u) 1.0,REV=1.1
Select package(s) you wish to process (or 'all' to process
all packages). (default: all) [?,??,q]:
```

Step 3 Press **Enter** to install all the packages. The following text appears:

```
Processing package instance <SUNWtsalm from </cdrom/netrat_11xx_1_0

TS91 Alarm and Monitor Manpages
(sparc.sun4u) 1.0,REV=1.1
      Copyright 1997 Sun Microsystems, Inc. All Rights Reserved.
            Manufactured in the United States of America.
2550 Garcia Avenue, Mountain View, California, 94043-1100 U.S.A.

Copyright 1997 Sun Microsystems Inc. Tous droits reserves.
Fabrique aux Etats-Unis, 2550 Garcia Avenue, Mountain View, Californie
94043-1100 USA
...
Installing TS91 Alarm and Monitor Manpages as <SUNWtsalm
...
Installation of <SUNWtsalm was successful.

Processing package instance <SUNWtsalr from </cdrom/netrat_11xx_1_0

TS91 Alarm and Monitor driver
(sparc.sun4u) 1.0,REV=1.1
      Copyright 1997 Sun Microsystems, Inc. All Rights Reserved.
      Manufactured in the United States of America.
      2550 Garcia Avenue, Mountain View, California, 94043-1100 U.S.A.
Do you want to continue with the installation of <SUNWtsalr [y,n,?]
```

Step 4 Type **y** and press **Enter** to continue the installation. The following text appears:

```
    Installing TS91 Alarm and Monitor driver as <SUNWtsalr
    ...
    Installation of <SUNWtsalr was successful.

    Processing package instance <SUNWtsalu from </cdrom/netrat_11xx_1_0

    TS91 Alarm and Monitor Utilities
    (sparc.sun4u) 1.0,REV=1.1
          Copyright 1997 Sun Microsystems, Inc. All Rights Reserved.
                Manufactured in the United States of America.
    2550 Garcia Avenue, Mountain View, California, 94043-1100 U.S.A.

    ...
    Installation of <SUNWtsalu was successful.

    The following packages are available:
      1  SUNWtsalm     TS91 Alarm and Monitor Manpages
                       (sparc.sun4u) 1.0,REV=1.1
      2  SUNWtsalr     TS91 Alarm and Monitor driver
                       (sparc.sun4u) 1.0,REV=1.1
      3  SUNWtsalu     TS91 Alarm and Monitor Utilities
                       (sparc.sun4u) 1.0,REV=1.1

    Select package(s) you wish to process (or 'all' to process
    all packages). (default: all) [?,??,q]:
```

Step 5 Type **q** to quit the installation.

Step 6 Eject the CD-ROM from the drive by typing each of the following commands at a # prompt and pressing **Enter**:

```
# cd /
# eject
```

This completes the installation of the Sun Solaris 2.6 software and patches.

If you have an asynchronous serial port card, continue to the "Installing the SAI/P Drivers" section on page 6-19.

To add an optional second Ethernet interface, continue to the "Configuring a Second Ethernet Interface" section on page 6-21.

If you have a second disk drive to configure, also see the "Configuring a Second Disk Drive" section on page 6-21.

If neither of these cases apply to your installation, continue with the next step in your chosen upgrade procedure in Chapter 1, "Solution-Level Upgrade Procedures."

If you have questions or need assistance, see the "Obtaining Technical Assistance" section on page xviii.

Installing the SAI/P Drivers

To install the Serial Asynchronous Interface/PCI (SAI/P) drivers if you have an asynchronous serial port card, perform the following steps:

Step 1 Insert the Cisco MGC Installation CD into the CD-ROM drive. Install the SAI/P Software by entering the following commands at the # prompt:

```
# cd /cdrom/cdrom0/saip_2.0_u1/Solaris_2.6/Packages
# pkgadd -d .
```

The following screen is displayed along with copyright and trademark information:

```
The following packages are available:
  1  SUNWsaip      Serial Asynchronous Interface Driver (PCI)
                   (sparc) 2.0,REV=1998.10.19
  2  SUNWsaipu     Serial Asynchronous Interface Utilities (PCI)
                   (sparc) 2.0,REV=1998.10.19

Select package(s) you wish to process (or 'all' to process
all packages). (default:all) [?,??,q]:
```

Step 2 Select **y** and press **Enter** to install all the packages. The following screen is displayed:

```
Processing package instance <SUNWsaip> from
</cdrom/sun_saip/saip_2.0_u1/Solaris_7/Packages>

Serial Asynchronous Interface Driver (PCI)
(sparc) 2.0,REV=1998.10.19
Copyright 1998 Sun Microsystems, Inc. All rights reserved.
Using </> as the package base directory.
## Processing package information.
## Processing system information.
```

```
   9 package pathnames are already properly installed.
## Verifying package dependencies.
## Verifying disk space requirements.
## Checking for conflicts with packages already installed.
## Checking for setuid/setgid programs.

This package contains scripts which will be executed with super-user
permission during the process of installing this package.

Do you want to continue with the installation of <SUNWsaip> [y,n,?] y
```

Step 3 Select **y** and press **Enter** to continue. The following screen is displayed:

```
Installing Serial Asynchronous Interface Driver (PCI) as <SUNWsaip>

## Installing part 1 of 1.
/etc/init.d/saip
/etc/opt/SUNWconn/bin/saipconfig <symbolic link>
/etc/opt/SUNWconn/bin/saipd <symbolic link>
/etc/opt/SUNWconn/saip/bin/saipconfig
.
.
.


Installation of <SUNWsaipu> was successful.

The following packages are available:
  1  SUNWsaip      Serial Asynchronous Interface Driver (PCI)
                   (sparc) 2.0,REV=1998.10.19
  2  SUNWsaipu     Serial Asynchronous Interface Utilities (PCI)
                   (sparc) 2.0,REV=1998.10.19

Select package(s) you wish to process (or 'all' to process
all packages). (default:all) [?,??,q]:q
```

Step 4 Select **q** and press **Enter** to quit the installation.

Step 5 Eject the CD-ROM from the drive:

```
# cd /
# eject
```

Step 6 Reboot the system by entering the following command and pressing **Enter**:

```
# reboot -- -r
```

To add an optional second Ethernet interface, continue to the “Configuring a Second Ethernet Interface” section on page 6-21.

If you have a second disk drive to configure, also see the “Configuring a Second Disk Drive” section on page 6-21.

If neither of these cases apply to your installation, continue with the next step in your chosen upgrade procedure in Chapter 1, “Solution-Level Upgrade Procedures.”

If you have questions or need assistance, see the “Obtaining Technical Assistance” section on page xviii.

Configuring a Second Ethernet Interface

A second Ethernet interface is optional to the base configuration. The second interface must be configured separately by following the steps below:

Step 1 Edit the hosts file in /etc to add the IP address and host name of the second Ethernet interface.

Step 2 Save the file and close it.

Step 3 Create a new file named hostname.hme1 in directory /etc. On on the first (and only) line, place the host name for the second Ethernet interface.

Step 4 If the IP address of the second Ethernet interface is on a different network than that of the first Ethernet interface, and this network for the second Ethernet interface has a subnet mask, edit the netmasks file in /etc to add the netmask for the new network. Follow the example in the header of the file.

Step 5 Reboot the system by entering the following command and pressing **Enter**:

```
# reboot -- -r
```

Step 6 When the machine finishes rebooting, log in as root.

Step 7 Type the following command and press **Enter**:

```
# ifconfig -a
```

Verify that the new interface, hme1, appears in the output text that looks similar to the following:

Note IP addresses are for demonstration purposes only. Actual addresses differ in each application.

```
lo0: flags=849<UP,LOOPBACK,RUNNING,MULTICAST> mtu 8232
        inet 127.0.0.1 netmask ff000000
hme0: flags=863<UP,BROADCAST,NOTRAILERS,RUNNING,MULTICAST> mtu 1500
        inet 172.24.235.53 netmask ffffff00 broadcast 172.24.235.255
        ether 8:0:20:9a:76:6c
hme1: flags=863<UP,BROADCAST,NOTRAILERS,RUNNING,MULTICAST> mtu 1500
        inet 172.24.237.53 netmask ffffff00 broadcast 172.24.237.255
        ether 8:0:20:9a:76:6c
```

This completes the configuration of a second Ethernet interface.

If you have a second disk drive to configure, see the “Configuring a Second Disk Drive” section on page 6-21. Otherwise, continue with the next step in your upgrade procedure in Chapter 1, “Solution-Level Upgrade Procedures.”

If you have questions or need assistance, see the “Obtaining Technical Assistance” section on page xviii.

Configuring a Second Disk Drive

- If you have a second disk installed that you want to use as mirror of the first in order to increase the availability of the system, go to the “Installing the Volume Manager” section on page 6-22.
- If you have a second disk installed that you want to use for log and spool systems in order to increase performance, go to the “Installing Log and Spool File Systems” section on page 6-29.

Installing the Volume Manager

Note If you are installing the operating system software on a single-host system, skip this section.

This section provides instructions for installing the Sun Enterprise Volume Manager 2.6 software, configuring the hard disk drives, and mirroring the operating system. Disk mirroring increases the availability of your system and prevents data loss. You can off load log and spool tasks to the second disk.

Caution This section should be used only for mirroring the boot disk drive onto a second disk *instead of* using the second drive for the log and spool file systems.

Use the second disk drive either for mirroring the first disk drive only, or for log and spool file systems only; do not use it for both.

This section contains the following procedures:

- "Installing the Sun StorEdge Volume Manager" section on page 6-22
- "License Key Entry and Boot Disk Encapsulation" section on page 6-25
- "Mirroring the Boot Disk" section on page 6-28

Installing the Sun StorEdge Volume Manager

To install the Sun StorEdge Volume Manager software and patch, complete the following steps:

Step 1 Load the Cisco MGC Software CD in the CD-ROM drive.

Step 2 Log in as root.

Step 3 Install the Volume Manager software patches by entering the following command:

```
pkgadd -d cdrom/cdrom0/solaris_patches/CSCOh006.pkg
```

The following text appears:

```
The following packages are available:
1  CSCOh006     Virtual Switch Controller Volume Manager 2.6 package installation and
patches
                  (sparc) TJB_ELAN_2000_01_04_23_16_GMT
Select package(s) you wish to process (or 'all' to process
all packages). (default: all) [?,??,q]:
```

Step 4 Press **Enter** to accept the default response of all. The following text appears:

```
Processing package instance <CSCOh006> from </var/tmp/CSCOh006.pkg>

Virtual Switch Controller Volume Manager 2.6 package installation and patches
(sparc) TJB_ELAN_2000_01_04_23_16_GMT
Cisco System, Inc.

The selected base directory </opt/sun_install> must exist before
installation is attempted.
```

```
Do you want this directory created now [y,n,?,q]
```

Step 5 Type **y** and press **Enter** to create this directory. The following text appears:

```
Using </opt/sun_install> as the package base directory.
## Processing package information.
## Processing system information.
   1 package pathname is already properly installed.
## Verifying disk space requirements.
## Checking for conflicts with packages already installed.

The following files are already installed on the system and are being
used by another package:
* /opt/sun_install <attribute change only>

* - conflict with a file which does not belong to any package.

Do you want to install these conflicting files [y,n,?,q]
```

Step 6 Type **y** and press **Enter** to continue installation. The following text appears:

```
## Checking for setuid/setgid programs.

This package contains scripts which will be executed with super-user
permission during the process of installing this package.

Do you want to continue with the installation of <CSCOh006> [y,n,?]
```

Step 7 Type **y** and press **Enter** to continue installation. The following text appears:

```
Installing Virtual Switch Controller Volume Manager 2.6 package installation and patches
as <CSCOh006>

## Executing preinstall script.
Platform is SUNW,Ultra-80

NOTICE: Architecture checks passed

## Installing part 1 of 1.
/opt/sun_install/installVM
/opt/sun_install/install_rootdg
/opt/sun_install/install_vscdg
/opt/sun_install/removeVM
/opt/sun_install/remove_rootdg
/opt/sun_install/remove_vscdg
/var/tmp/106606-02.tar.Z
[ verifying class <none> ]
## Executing postinstall script.

!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!                                                            !!
!!  You must now change directories to /opt/sun_install and   !!
!!  run the installVM script as root.                         !!
!!                                                            !!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!


Installation of <CSCOh006> was successful.
```

Step 8 Enter the following command to run the VM script:

```
# ./installVM
```

The CD-ROM is ejected from the machine. The following text appears:

```
Install the "Sun StorEdge Volume Manager 2.6 Software" CD into the CD-ROM driver
Press Enter when ready
```

Step 9 Insert the Sun StorEdge Volume Manager CD into the CD-ROM drive.

Step 10 Press **Enter** to continue installation. The following text appears:

```
    Sun StorEdge Volume Manager
    (sparc) 2.6,REV=2.5.3
    Copyright 1998 Sun Microsystems, Inc. All rights reserved.

    Copyright (c) 1990-1997 VERITAS Software Corporation.
    ALL RIGHTS RESERVED.
    THIS SOFTWARE IS THE PROPERTY OF AND IS LICENSED BY VERITAS SOFTWARE,
    AND/OR ITS SUPPLIERS.
    ## Processing package information.
## Processing system information.
   10 package pathnames are already properly installed.
## Verifying package dependencies.
## Verifying disk space requirements.
## Checking for conflicts with packages already installed.

The following files are already installed on the system and are being
used by another package:
  /etc <attribute change only>

Do you want to install these conflicting files [y,n,?,q]
```

Step 11 Type **y** and press **Enter** to continue installation. The following text appears:

```
## Checking for setuid/setgid programs.

The following files are being installed with setuid and/or setgid
permissions:
  /usr/sbin/vxprint <setuid root>

Do you want to install these as setuid/setgid files [y,n,?,q]
```

Step 12 Type **y** and press **Enter** to continue installation. The following text appears:

```
This package contains scripts which will be executed with super-user
permission during the process of installing this package.

Do you want to continue with the installation of <SUNWvxvm> [y,n,?]
```

Step 13 Type **y** and press **Enter** to continue installation. The following text appears:

```
    Copyright (c) 1990-1997 VERITAS Software Corporation.
    ALL RIGHTS RESERVED.
    THIS SOFTWARE IS THE PROPERTY OF AND IS LICENSED BY VERITAS SOFTWARE,
    AND/OR ITS SUPPLIERS.
    Using </opt> as the package base directory.
    ## Processing package information.
    ## Processing system information.
    ## Verifying package dependencies.
    ## Verifying disk space requirements.
    ## Checking for conflicts with packages already installed.
    ## Checking for setuid/setgid programs.
    This package contains scripts which will be executed with super-user
    permission during the process of installing this package.

Do you want to continue with the installation of <SUNWvxva> [y,n,?]
```

Step 14 Type **y** and press **Enter** to continue installation. The following text appears:

```
Installation of <SUNWvmman> was successful.
Ejecting CDROM
Changed to /var/tmp directory
Uncompressing 106606-02 ...
Extracting 106606-02 ...
Extraction of patch 106606-02 successful
Installing 106606-02 ...
Create vxassist file
Create vxaltstale file
Edit S95vxvm-recover script

!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!! The system must be rebooted before running 'vxinstall' !!
!! as root to continue the Volume Manager installation.   !!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!

Do you want to reboot now (y/n)?
```

Step 15 Type **y** and press **Enter** to reboot. The following text appears:

```
REBOOTING
#
INIT: New run level: 6
The system is coming down. Please wait.
System services are now being stopped.
Print services stopped.
Stopping the syslog service.
syslogd: going down on signal 15
Jan  6 12:56:21 snmpdx: received signal 15
The system is down.
```

This completes installation of the Sun StorEdge Volume Manager software and patch. Continue to the "License Key Entry and Boot Disk Encapsulation" section on page 6-25.

License Key Entry and Boot Disk Encapsulation

Note The Volume Manager key from Sun also comes with a RAID-5 key. Although RAID-5 provides another way to mirror or back up information, it is not necessary in this application.

Step 1 When the reboot is complete, log in as root and boot to the # prompt.

Step 2 Type the following command at the # prompt and press **Enter**:

```
# vxinstall
```

The following notice appears:

```
VxVM uses license keys to control access.  If you have a SPARCstorage
Array (SSA) controller or a Sun Enterprise Network Array (SENA) controller
attached to your system, then VxVM will grant you a limited use license
automatically.  The SSA and/or SENA license grants you unrestricted use
of disks attached to an SSA or SENA controller, but disallows striping
and RAID-5 on non-SSA and non-SENA disks.  If you are not running a
SPARCstorage Array controller, or a Sun Enterprise Network Array controller, then you must
obtain a license key to operate.
```

```
Licensing information:
 System host ID: 80c4d518
 Host type: SUNW,Ultra-80
 SPARCstorage Array or Sun Enterprise Network Array: No arrays found (license is required)
Are you prepared to enter a license key [y,n,q,?] (default: y)
```

Step 3 Press **Enter** to accept the default answer "yes." The following text appears:

```
Please enter your key:
```

Step 4 Type the key number, with spaces, and press **Enter**. The following text appears:

```
vrts:vxlicense: INFO: Feature name: CURRSET [95]
vrts:vxlicense: INFO: Number of licenses: 1 (non-floating)
vrts:vxlicense: INFO: Expiration date: Sun Jun 04 04:00:00 2006 (2340.6 days from now)
vrts:vxlicense: INFO: Release Level: 20
vrts:vxlicense: INFO: Machine Class: All
vrts:vxlicense: INFO: Key successfully installed in /etc/vx/elm/95.

Do you wish to enter another license key [y,n,q,?] (default: n)
```

Step 5 Press **Enter** to accept the default answer no. The following text appears:

```
Volume Manager Installation
Menu: VolumeManager/Install

  The Volume Manager names disks on your system using the controller
  and disk number of the disk, substituting them into the following
  pattern:
        c<controller>t<disk>d<disk>

  If the Multipathing driver is installed on the system then for the
  disk devices with multiple access paths, the controller number
  represents a multipath pseudo controller number. For example, if a
  disk has 2 paths from controllers c0 and c1, then the Volume Manager
  displays only one of them such as c0 to represent both the
  controllers.

  Some examples would be:

        c0t0d0  - first controller, first target, first disk
        c1t0d0  - second controller, first target, first disk
        c1t1d0  - second controller, second target, first disk

The Volume Manager has detected the following controllers on your system:

        c0:

Hit RETURN to continue.
```

Step 6 Press **Enter** to continue. The following text appears:

```
Volume Manager Installation
Menu: VolumeManager/Install

  You will now be asked if you wish to use Quick Installation or
  Custom Installation.  Custom Installation allows you to select how
  the Volume Manager will handle the installation of each disk
  attached to your system.

  Quick Installation examines each disk attached to your system and
  attempts to create volumes to cover all disk partitions that might
  be used for file systems or for other similar purposes.

  If you do not wish to use some disks with the Volume Manager, or if
  you wish to reinitialize some disks, use the Custom Installation
  option Otherwise, we suggest that you use the Quick Installation
  option.
Hit RETURN to continue.
```

Step 7 Press **Enter** to continue. The following text appears:

```
Volume Manager Installation Options
Menu: VolumeManager/Install

 1      Quick Installation
 2      Custom Installation

 ?      Display help about menu
 ??     Display help about the menuing system
 q      Exit from menus

Select an operation to perform:
```

Step 8 Type 2 and press **Enter** to continue. The following text appears:

```
Volume Manager Custom Installation
Menu: VolumeManager/Install/Custom

  The c0t0d0 disk is your Boot Disk.  You can not add it as a new
  disk.  If you encapsulate it, you will make your root filesystem
  and other system areas on the Boot Disk into volumes.  This is
  required if you wish to mirror your root filesystem or system
  swap area.

Encapsulate Boot Disk [y,n,q,?] (default: n)
```

Step 9 Type **y** and press **Enter** to continue. The following text appears:

```
Enter disk name for c0t0d0 [<name>,q,?] (default: rootdisk)
```

Step 10 Type **rootdiska** and press **Enter** to continue. The following text appears:

```
The c0t0d0 disk has been configured for encapsulation.

Hit RETURN to continue.
```

Step 11 Press **Enter** to continue. The following text appears:

```
Volume Manager Custom Installation
Menu: VolumeManager/Install/Custom/c0
Generating list of attached disks on c0....

<excluding root disk c0t0d0

  The Volume Manager has detected the following disks on controller c0:

  c0t1d0

Hit RETURN to continue.
```

Step 12 Press **Enter** to continue. The following text appears:

```
Installation options for controller c0
Menu: VolumeManager/Install/Custom/c0

 1      Install all disks as pre-existing disks. (encapsulate)
 2      Install all disks as new disks. (discards data on disks!)
 3      Install one disk at a time.
 4      Leave these disks alone.
 ?      Display help about menu
 ??     Display help about the menuing system
 q      Exit from menus

Select an operation to perform:
```

Step 13 Type **4** to leave the disks alone and press **Enter** to continue. The following text appears:

```
Volume Manager Custom Installation
Menu: VolumeManager/Install/Custom

The following is a summary of your choices.
c0t0d0  Encapsulate
Is this correct [y,n,q,?] (default: y)
```

Step 14 Press **Enter** to accept the default answer, "yes," and continue.

```
The system now must be shut down and rebooted in order to continue
the reconfiguration.

Shutdown and reboot now [y,n,q,?] (default: n)
```

Step 15 Type **y** and press **Enter** to shut down and reboot the system.

Step 16 Wait for the computer to shut down and reboot twice, then proceed to the next section.

This completes license key entry and boot disk encapsulation. Continue to the "Mirroring the Boot Disk" section on page 6-28.

Mirroring the Boot Disk

Step 1 After the system has rebooted twice, log in as root at the # prompt and run the install_rootdg script as shown below:

```
#  cd /opt/sun_install
# ./install_rootdg
```

Note This process takes approximately 30 minutes to run and does not require user intervention.

```
# cd /opt/sun_install
# ./install_rootdg
The following is displayed.
Determine the device names for the disks
Platform is SUNW,Ultra-60
A-DSK0: c0t0d0
B-DSK0: c0t1d0
Initialize device c0t1d0
Succeeded
Add rootdiskb to rootdg, device is c0t1d0
Succeeded
Mirror all the volumes of A-DSK0 to B-DKS0 and make root
bootable
Mirroring root to rootdiskb
Success
Mirroring var to rootdiskb
```

```
Success
Mirroring opt to rootdiskb
Success
Mirroring swap to rootdiskb
Success
Mirroring usr to rootdiskb
Success
```

Step 2 At the # prompt, type **init 6** and press **Enter** to reboot the system.

```
# init 6
```

Note After you install Volume Manager, you will see warning messages similar to the example below every time you boot up the server. However, these messages are acceptable and do not affect the operation of the SC host.

```
>>WARNING: forceload of drv/scsi failed
>>WARNING: forceload of drv/ssd failed
>>WARNING: forceload of drv/sf failed
>>WARNING: forceload of drv/pln failed
>>WARNING: forceload of drv/soc failed
>>WARNING: forceload of drv/socal failed
```

This completes configuration of a second disk drive to use for disk mirroring.

If you use this second disk drive to hold log file and spool file systems, proceed to the “Installing Log and Spool File Systems” section on page 6-29. Otherwise, continue with the next step in your upgrade procedure in Chapter 1, “Solution-Level Upgrade Procedures.”

If you have questions or need assistance, see the “Obtaining Technical Assistance” section on page xviii.

Installing Log and Spool File Systems

Note Follow the procedures in this section only if you are using a second disk drive for the log and spool file systems, and therefore are *not* mirroring the second disk drive.

Installing log file and spool file systems is accomplished by performing the following steps:

Step 1 Insert the Cisco MGC Software CD into the CD-ROM drive.

Step 2 Type the following command at the # prompt and press **Enter**:

```
pkgadd -d cdrom/cdrom0/solaris_patches/CSCOh005.pkg
```

The following text appears:

```
The following packages are available:
  1  CSCOh005     Media Gateway Controller VSC log and spool package
                  (sparc) TJB_ELAN_1999_10_28_20_36_GMT

Select package(s) you wish to process (or 'all' to process
all packages). (default: all) [?,??,q]:
```

Step 3 Press **Enter** to accept the default answer **all**. The following text appears:

```
Processing package instance <CSCOh005 from </var/tmp/CSCOh005.pkg

Media Gateway Controller VSC log and spool package
(sparc) TJB_ELAN_1999_10_28_20_36_GMT
Cisco System, Inc.
Using </opt/sun_install as the package base directory.
## Processing package information.
## Processing system information.
   1 package pathname is already properly installed.
## Verifying disk space requirements.
## Checking for conflicts with packages already installed.
## Checking for setuid/setgid programs.

This package contains scripts which will be executed with super-user
permission during the process of installing this package.

Do you want to continue with the installation of <CSCOh005 [y,n,?]
```

Step 4 Type **y** and press **Enter** to continue. The following text appears:

```
    Installing Media Gateway Controller VSC log and spool package as
    <CSCOh005>

    ## Executing preinstall script.
    Platform is SUNW,Ultra-60

    NOTICE: Architecture checks passed

    ## Installing part 1 of 1.
    /opt/sun_install/format_log_spool.cmd
    /opt/sun_install/install_log_spool
    [ verifying class <none ]
    ## Executing postinstall script.

    !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
    !!  !!
    !!  You must now change directories to /opt/sun_install and!!
    !!  run the install_log_spool script as root.            !!
    !!                                                       !!
    !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!

    Installation of <CSCOh005> was successful.
```

Step 5 Change directories to /opt/sun_install, then run the install_log_spool script, by typing each of the following commands at a # prompt and pressing **Enter**:

```
# cd /opt/sun_install
# ./install_log_spool
```

The following text appears:

```
Build partition table for c0t1d0 ...
Searching for disks...done
selecting c0t1d0
...
Adding entries to /etc/vfstab

Mounting /opt/CiscoMGC/var/log

Mounting /opt/CiscoMGC/var/spool
Success!!!
```

Where to Go Next

This completes the operating system installation. For more information about installing the Sun Solaris 2.6 operating system software and patches, refer to the Sun documentation that shipped with the product.

Continue with the next step in your chosen upgrade procedure in Chapter 1, “Solution-Level Upgrade Procedures.”

Upgrading Cisco SC2200 Software

Before beginning the upgrade, verify that you have the Cisco Media Gateway Controller Software Release 7 CD-ROM. (For Software Release 7.3(x), this is called the Cisco Telephony Controller Software Release 7 CD-ROM.)

Use the instructions in this section to install new software. If you have a simplex configuration, install the software on your server. If you have a high-availability configuration, install the software on the standby first.

Note Procedures for installing Software Release 7.3(x) differ from Software Release 7.4(x). Follow the instructions for the version you are installing.

This chapter contains the following sections:

Note Always consult the latest *Release Notes for Cisco Media Gateway Controller Software Release 7* (available from your Cisco representative) to make sure that you have the most current release of software and that no additional patches are required. If patches are required, consult the release notes for patch installation procedures.

Tip Many of the procedures in this chapter require using an editor such as vi to make changes to files. If you experience screen viewing problems, try the following:

- If you are not sure which shell you are using, enter the following commands:

```
TERM=xterm
export TERM
stty rows 24
```

- If you are using a Bourne shell, enter the **TERM=vt100; export TERM** command.
- If you are using a C shell, enter the **setenv TERM vt100** command.

Identifying the Active Configuration

Identify and make note of the name of the active configuration by performing the following steps:

Step 1 Log in to the SC host to be upgraded and enter the following UNIX command to access the configuration library:

```
config-lib
```

The system returns a response similar to the following.

```
The Configuration File Library Main Menu

1. List Configuration Versions in Library
2. Save Production to a new Library Version
3. Copy Library Version to Production
4. Remove Configuration Library Version
Enter Selection or 'q' to quit>
```

Step 2 Enter 1 at the prompt to list the configuration versions in the library.

At the bottom of the list, a configuration is identified as being the current production version. This is the name of your active configuration.

Removing a Previous Version of the Cisco Telephony Controller Software (Release 4 and Release 7.3(x))

Note If you are removing Software Release or 7.4, follow the instructions in the "Removing a Previous Version of the Cisco MGC Software (Release 7.4(x))" section on page 7-4.

Before upgrading the SC software, you must first uninstall the previous software version. To remove the Cisco telephony controller software, complete the following steps:

Step 1 Log in at the console as the root user.

Step 2 Insert the SC host software Version 7.3 CD-ROM into the CD-ROM drive and enter the following commands:

```
# cd /cdrom/cdrom0
# ./uninstall.sh
```

Step 3 The system asks if you want to use the supplied administrative file to perform an unattended package removal. This process removes all the packages automatically.

Timesaver If you do not accept the unattended removal, the system prompts you before removing each package individually.

Step 4 Type **y** (yes) and press **Enter** to accept unattended package removal. The system displays a list of packages as it removes them.

When package removal is finished, the following message appears:

```
Uninstallation log can be found in /tmp/uninstall.log.
```

Step 5 Enter the following command:

```
cd /etc
```

Step 6 Open the group file with your editor.

Step 7 Make sure that the "transpath" group is removed. This group must be removed in order to accept default software installation later.

Step 8 Save any changes to the group file and close it.

This completes the removal of the previous version of the telephony controller software. If you have questions or need assistance, see the "Obtaining Technical Assistance" section on page xviii.

Removing a Previous Version of the Cisco MGC Software (Release 7.4(x))

Before upgrading an existing release of the SC host software, you must first uninstall the previous software version.

Note If you are removing Software Release 4 or 7.3, follow the instructions in the "Removing a Previous Version of the Cisco Telephony Controller Software (Release 4 and Release 7.3(x))" section on page 7-3.

To remove the SC host software, complete the following steps:

Step 1 Log in at the console as the root user.

Step 2 Insert the SC host Software Version 7.4 CD-ROM into the CD-ROM drive and enter the following commands:

```
# ./uninstall.sh
```

Step 3 If you are upgrading from a previous version of software Release 7, answer **y** to the following prompt. If this is an initial installation, answer **n**:

```
If you answer no to the following question you will lose all new provisioning work.
Is the uninstall being done in order to upgrade to a new version of the software? [y]
[y,n,?,q]
```

Step 4 The system asks if you want to use the supplied administrative file to perform an unattended package removal. This process removes all the packages automatically.

Timesaver If you do not accept the unattended removal, the system prompts you before removing each package individually.

Step 5 Type **y** (yes) and press **Enter** to accept unattended package removal. The system displays a list of packages as it removes them.

When package removal is finished, the following message appears:

```
Uninstallation log can be found in /tmp/uninstall.log.
```

Step 6 Enter the following command:

```
cd /etc
```

Step 7 Open the group file with your editor.

Step 8 Make sure that the "transpath" and "mgcgrp" groups are removed. These groups must be removed in order to accept default software installation later.

Step 9 Save any changes to the group file and close it.

This completes the removal of the previous version of the SC host software. If you have questions or need assistance, see the "Obtaining Technical Assistance" section on page xviii.

Installing SC Software Release 7.3(x)

To install Software Release 7.3(x), follow these steps:

Note You must be logged in as root. Do not log in as another user and enter **su** to become root. Logging in as root might require use of a console connected to the SC host.

Step 1 Insert the SC host software Release 7.3(x) CD into the CD-ROM drive.

Step 2 To install the Release 7.3(x) software, enter the following commands:

```
# cd /cdrom/cdrom0
# ./install.sh
```

Step 3 The following prompt appears:

```
Use supplied admin file for unattended install? [n] [y,n,?,q]
```

Answer **y** to perform an unattended installation. If you answer n, you must answer prompts and press **Enter** for each package that is installed.

Note The initial installation takes approximately 1 hour.

Step 4 The following prompt appears:

```
Install Telephony Configuration Manager (TCM) package? [n] [y,n,?,q]
```

Answer **y** if you want to install the CMM on this host.

Tips To install the CMM on a separate host, follow the steps in "Installing the CMM" section on page 7-10.

Step 5 The following prompt appears:

```
Base directory for CMM (default /opt/VSCprov) [?,q]
```

Press **Enter** to accept the default directory, /opt/VSCprov. We recommend that you not change the directory.

Step 6 The following prompt appears:

```
The CSCOgu000 utilities package must be installed prior to other components but has not
been detected on your system.
Would you like to install it now? [y] [y,n,?,q]
```

Answer **y** to install the utilities package. This package must be installed before you install the rest of the software.

Caution Before accepting the default user ID and group ID as recommended in the step below, you must make sure old transpath IDs are deleted in the /etc/group directory. We recommend that the group directory itself be deleted.

Step 7 The following prompts appear:

```
Enter transpath user name [transpath]
Enter transpath UID [20000]
Enter transpath group name [transpath]
```

We recommend that you accept the default values (by pressing **Enter**).

You can, however, specify a different user ID and a group ID. If the ID you specify already exists on the system, the corresponding ID is determined and reused, or you are prompted to enter another ID.

Caution No validation is performed on the IDs you enter. If you enter an invalid ID, the utilities package does not add any accounts.

The system returns a message that the CSCOgu000 utilities package was successfully installed.

Step 8 Rebooting after a successful utilities package installation might or might not be necessary, based on your system configuration.

If a reboot is *not* required, the installation continues uninterrupted. When the installation is finished, continue to Step 9.

If a reboot *is* required, perform the following steps when prompted:

a. Type the command displayed on the screen and press **Enter**.

Note If the command shown on the screen does not work, you can enter the **/usr/sbin/reboot** command to reboot the system.

b. After the reboot finishes, restart install.sh to install the remaining packages. To restart install.sh, type each of the following commands at the # prompt and press **Enter**:

```
# cd /cdrom/cdrom0
# ./install.sh
```

c. When the package installation is finished, continue to Step 9.

Step 9 Press **Enter** to install the selected package. The installation script installs the drivers and reboots the host.

This completes installing the SC software.

Note When installing the software, only the active configuration files (located in /opt/TransPath/etc) are migrated. If you have older configurations you need to migrate, see the “Migrating Inactive SC Host Configurations” section on page 7-63.

Tip If you did not review your MML names in the components.dat and properties.dat files before beginning the upgrade, and your MML names did not conform to the new standards, you received a migration error. To correct the situation:

Step 1 Uninstall the failed package CSCOgc001 by entering the **pkgrm CSCOgc001.pkg** command. Answer **Y** to the prompts.

Step 2 Refer to the "Reviewing Your Components.dat and Properties.dat Files for Potential Problems" section on page 1-3 for instructions on editing your MML names.

Step 3 Reinstall the package by changing to the /cdrom/cdrom0/APPLICATIONS directory and entering the **pkgadd -d CSCOgc001.pkg** command.

Installing SC Software Release 7.4(x)

To install Software Release 7.4(x), follow these steps:

Note You must be logged in as root. Do not log in as another user and enter **su** to become root. Logging in as root might require use of a console connected to the SC host.

Step 1 Log in as root and go to the # prompt.

Step 2 Enter the following command:

```
cd /etc
```

Step 3 Open the password file with your editor.

Step 4 Check that /opt/TransPath does not appear in the path of any user; if it does, change the path to /opt/CiscoMGC.

Step 5 Save any changes to the password file.

Step 6 Close the password file.

Step 7 Insert the SC host Software Release 7.4(x) CD into the CD-ROM drive.

Caution If you are upgrading to a new software release, you must first copy the new software from the CD-ROM to an appropriate directory in your system (for example, create a directory as root user under **/opt**), then perform the installation from that directory. This step prevents possible CD-ROM ejection problems.

When the upgrade has successfully completed, it is strongly recommended that you delete the software you copied from the CD-ROM to your directory, to avoid running out of disk space.

Step 8 To install the Release 7.4(x) SC host software, enter the following command:

```
# ./install.sh
```

Step 9 The following prompt appears:

```
Use supplied admin file for unattended install? [n] [y,n,?,q]
```

Answer **y** to perform an unattended installation. If you answer n, you must answer prompts and press **Enter** for each package that is installed.

Note The initial installation takes approximately 1 hour.

Step 10 The following prompt appears:

```
Install Cisco Media Gateway Controller Manager (CMM/Toolkit) package?
[n] [y,n,?,q]
```

Answer **y** if you want to install the CMM and the Toolkit applications on this host.

Tips To install the CMM on a separate host, follow the steps in the “Installing the CMM” section on page 7-10.

Step 11 The following prompt appears:

```
Base directory for CMM/Toolkit (default /opt/CMM) [?,q]
```

Press **Enter** to accept the default directory, /opt/CMM. We recommend that you not change the directory.

Step 12 The following prompt appears:

```
The CSCOgu000 utilities package must be installed prior to other components but has not
been detected on your system.
Would you like to install it now? [y] [y,n,?,q]
```

Answer **y** to install the utilities package. This package must be installed before you install the rest of the software.

Caution Before accepting the default user ID and group ID as recommended in the step below, you must make sure old transpath IDs are deleted in the /etc/group directory. We recommend that the group directory itself be deleted.

Step 13 The following prompts appear:

```
Base directory for CiscoMGC (default /opt/CiscoMGC) [?,q]
Enter CiscoMGC user name [mgcusr]
Enter CiscoMGC UID [20000]
Enter CiscoMGC group name [mgcgrp]
Enter CiscoMGC GID [2000]
```

We recommend that you accept the default values for each of the prompts (by pressing **Enter**).

You can, however, specify a different user ID and a group ID. If the ID you specify already exists on the system, the corresponding ID will be determined and reused, or you will be prompted to enter another ID.

Caution No validation is performed on the IDs you enter. If you enter an invalid ID, the utilities package does not add any accounts.

The system returns a message that the CSCOgu000 utilities package was successfully installed.

Step 14 Rebooting after a successful utilities package installation might or might not be necessary, based on your system configuration.

Note Rebooting may take about 5 minutes.

If a reboot is *not* required, the installation continues uninterrupted. When the installation is finished, continue to Step 15.

If a reboot *is* required, perform the following steps when prompted:

a. Type the command displayed on the screen and press **Enter**.

Note If the command shown on the screen does not work, you can enter the **/usr/sbin/reboot** command to reboot the system.

b. After the reboot finishes, restart install.sh to install the remaining packages. To restart install.sh, type each of the following commands at the # prompt and press **Enter**:

```
# ./install.sh
```

c. The following prompts display:

```
Use supplied admin file for unattended install? [n] [y,n,?,q]
Install Cisco Media Gateway Controller Manager (CMM/Toolkit) package? [n] [y,n,?,q]
```

d. Type **y** for each of the prompts and press **Enter**.

e. When the package installation is finished, continue to Step 15.

Step 15 The system checks the memory and CPUs in the host. If you do not have enough memory or CPUs, a caution appears. You will get the Maximum Sustained/High Calls prompt, but it is possible that you will not get a warning on host resources.

After the check is complete, the following prompt appears:

```
Configure System for (1) Maximum Sustained Calls (2) High Call Throughput
Enter 1 or 2 or q to quit
```

Note Options 1 and 2 are performance tuning options that allow optimizing certain parameters and settings on the system for better performance, based on your system requirements. This choice should have been resolved when Cisco analyzed your system requirements.

Enter **1** or **2** to choose the option you want and press **Enter**.

Step 16 Press **Enter** to install the selected package. The installation script installs the drivers and reboots the host.

This completes installing the SC software.

Note When installing the software, only the active configuration files (located in /opt/CiscoMGC/etc) are migrated. If you have older configurations you need to migrate, see the "Migrating Inactive SC Host Configurations" section on page 7-63.

Tip If you did not review your MML names in the components.dat and properties.dat files before beginning the upgrade, and your MML names did not conform to the new standards, you received a migration error. To correct the situation:

Step 1 Uninstall the failed package CSCOgc001 by entering the **pkgrm CSCOgc001.pkg** command. Answer **Y** to the prompts.

Step 2 Refer to the "Reviewing Your Components.dat and Properties.dat Files for Potential Problems" section on page 1-3 for instructions on editing your MML names.

Step 3 Reinstall the package by changing to the /cdrom/cdrom0/APPLICATIONS directory and entering the **pkgadd -d CSCOgc001.pkg** command.

Installing Patches for the SC Software

There may be new patches available for your new SC software. Check the following URL for the latest patches:

http://www.cisco.com/kobayashi/sw-center/sw-voice.shtml

Click on the link for the software version of the Cisco Media Gateway Controller software that you just installed. The README files contain information about installing the patches. Download the files you need and follow the README file instructions.

For more information on patches for your release of the SC software, refer to the *Release Notes for the Cisco Media Gateway Controller Software Release 7*.

Installing a GUI Provisioning Tool on a Separate Server

You can install the GUI provisioning tools for the Cisco SC2200 on separate servers. The procedures to install the various GUI provisioning tools are described in the following sections:

- Installing the CMM, page 7-10
- Installing the Voice Service Provisioning Tool, page 7-11

Note The Voice Services Provisioning Tool (VSPT) must be installed on a separate server than the SC software.

Installing the CMM

You can install the CMM on a separate server than the SC software. To install only the CMM, perform the following steps:

Step 1 Insert the Cisco Media Gateway Controller Release 7 CD-ROM into the CD-ROM drive of the separate server.

Step 2 Change to the directory containing the CD-ROM by entering the following:

```
cd /cdrom/cdrom0
```

Step 3 Enter the following command:

```
./install-cmm-tool.sh
```

Answer **yes** to the onscreen prompts.

This completes installing the CMM on a separate host. Proceed to the "Configuring SNMP Support Resources" section on page 7-13.

Installing the Voice Service Provisioning Tool

The Voice Service Provisioning Tool (VSPT) is a graphical configuration/provisioning tool that enables you to create or modify configuration files across multiple devices such as MGCs and Cisco Media Gateways. If you are a registered Cisco.com user, you can download the VSPT from the Cisco website. For more information on VSPT, see *Cisco Voice Services Provisioning Tool Users Guide*.

The following files are located on the VSPT:

Table 7-1 Voice Service Provisioning Tool Installation CD Files

File	Description
setup	Installation script
setup.class	Install Shield installation class file
classes/	Voice Service Provisioning Tool class and property files
jre/	Java Runtime Environment

Prerequisites

To install the VSPT, you must have the following:

- Sun Sparc station running Solaris 2.6 or greater

Note Running the VSPT on the same host as the MGC can adversely impact performance. Cisco recommends using a separate server.

- Root user access
- Disk Space:
  - Approximately 20 MBs of disk space for installation
  - Directory /var/opt/data/:

    Approximately 1 MB for each configuration

    Approximately 1 MB for each configuration snapshot
  - Directory /var/opt/log/:

    Approximately 0.5 MB for each deployment

- RAM:
  - Minimum: 128 MBs
  - Recommended: 256 MBs or greater
- Swap space:
  - Minimum: 128 MBs
  - Recommended: 256 MBs or greater

Upgrading VSPT Software

If you have an older version of VSPT already installed (such as VSPT Version 1.1) and you are upgrading to VSPT Version 1.5, the existing VSPT data is automatically migrated to VSPT version 1.5; you do not need to uninstall the older version. However, if an incremental version is detected during the installation you will be prompted to uninstall the older version (for example, Version 1.5.1 cannot co-exist with Version 1.5.2 and must first be uninstalled).

To uninstall the software:

Note Since the uninstall directory and files are removed during uninstall, **do not** run the uninstall script from within the /opt/CSCOspgw directory.

Step 1 Enter the following commands:

```
su -root
cd /
/opt/CSCOspgw/uninstall/uninstall
```

The uninstallation process removes all files and directories created by the installation process. If a directory contains a file that was not created during the installation process, it is not removed and is logged in the uninstall.log file. This might occur in the data and logs directories.

Step 2 Proceed with the VSPT software installation (see Installing the VSPT Software, page 7-12).

Installing the VSPT Software

To install VSPT, follow the procedures listed below:

Step 1 Download the software from the following Cisco website:

http:/www/cisco.com/cgi-bin/tablebuild.pl/vspt

Note You must be a registered Cisco.com user to download this software.

Step 2 You will be prompted through the installation process.

This completes the VSPT software installation. If you have questions or need assistance, see the "Obtaining Technical Assistance" section on page xviii.

Configuring SNMP Support Resources

The Cisco MGC software includes a Simple Network Management Protocol (SNMP) agent subsystem that provides an alarm management interface on the SC host. It uses SNMP to report events, or traps (such as alarms), to your SNMP Manager and to provide access to the Cisco MGC Management Information Base (MIB).

The SNMP agent subsystem reports the following event categories to your SNMP Manager:

1. Communications
2. Quality of Service
3. Processing
4. Equipment
5. Environment

In a continuous-service or high-availability configuration, the SNMP agent subsystem runs on both the active and standby Cisco MGCs.

Note SNMP MIB measurements are only valid only on the active Cisco MGC. They are not replicated on the standby Cisco MGC.

To configure the SNMP resources, complete the following steps:

Step 1 Log in to the active Cisco MGC as root and change to the /etc directory using the following UNIX command:

```
cd /etc
```

Step 2 Verify that the name in the nodename file (using the **more nodename** UNIX command) matches a host name or nickname in the hosts file.

Note Entries in the hosts file are in the following format: *IP_address host_name nickname*.

If the names match, proceed to Step 4. Otherwise, proceed to Step 3.

Step 3 Use a text editing utility, such as vi, to edit the nodename file and enter the host name of this Cisco MGC.

Save your changes and exit the utility when you are finished.

Step 4 Verify that the services file lists the following default SNMP ports using the following UNIX command:

```
more services
```

The following lines should display among other port entries:

```
snmp      161/udp
snmp-trap 162/udp
```

If the ports for SNMP are listed, proceed to Step 9. Otherwise, continue to Step 3.

Step 5 Edit the services file using a text editor such as vi to add these two lines for snmp and snmp-trap port information.

```
vi services
snmp 161/udp
snmp-trap 162/udp
```

Save your changes and exit the editor when you are finished.

Step 6 Verify that the file is properly edited using the following UNIX command:

```
more services
```

The following lines should display among other port entries (otherwise, repeat Step 3):

```
snmp      161/udp
snmp-trap 162/udp
```

Step 7 Verify that the SNMP process is running using the following UNIX command:

```
ps -ef | grep snmpd
```

Step 8 Stop the existing SNMP process using the following UNIX command. This command automatically restarts the SNMP process with a new ID.

```
kill -HUP process_ID
```

Where *process_ID* is the process ID number for the SNMP process, as identified in Step 5.

Step 9 Verify that the SNMP process is running using the following UNIX command:

```
ps -ef | grep snmpd
```

Step 10 Verify that the SNMP process is no longer generating errors by checking the snmpd.log. To do this, enter the following command:

```
more/tmp/snmpd.log
```

If no errors are found, this means the process is working and you can use the ports for SNMP configuration and trap generation.

Step 11 Using FTP, transfer the following MIBs (located in /opt/CiscoMGC/snmp) from the Cisco SC host to the machine on which the SNMP manager runs:

- CISCO-SMI.my
- v3-tgt.my
- tp.my
- provisioning.my
- measurement.my

Step 12 Load the MIBs into the SNMP manager (for example, you can use the **xnmnloadmib -load** command from HP OpenView).

Note See your SNMP manager documentation for more information. Cisco does not recommend a specific SNMP manager; however, this chapter gives examples using the Hewlett-Packard (HP) OpenView Network Node Manager.

```
HP OpenView Example:
    If you are using HP OpenView Network Node Manager as your SNMP manager, follow
    these procedures to load your MIB:
    (a) Select Options from the File Menu and choose Load/Unload MIBs:SNMP.
    (b) From the Load/Unload MIBs: SNMP window (on the lower left of your screen).
    (c) Click the Load... button.
    (d) From the "Load/Unload MIBs:SNMP /Load MIB from File" window, select the MIB to
    load (for example, tp.my).
    (e) Click OK.
```

Tip For more detailed information about configuring HP OpenView, see Appendix A, "HP OpenView Sample SNMP Configuration," in *Cisco Media Gateway Controller Software Release 7 Installation and Configuration Guide.*

Step 13 Connect the SNMP events to an event category to display the event. As Cisco MGC events are connected, you can alter the format of the event messages for easier viewing.

Note On many SNMP managers, event categories can be added so that customer-specific events can be mapped to corresponding categories.

```
HP OpenView Event Configuration Example:
    If you are using HP OpenView Network Node Manager, follow these procedures to
    configure an event:
    (a) Select Options from the File Menu and choose Event Configuration.
    (b) From the Event Configuration window, in the Enterprise Identification list,
    select transpath.
    (c) In the Event Identification list, double click on each of the event types, one
    at a time.
    (d) If desired, change the event information display. To change the format of an
    event, from the Event Configurator / Modify Event window, enter a format in the
    Event Log Message Box to change the format and labels for received events of this
    type.

    The following example shows how an event can be reformatted using the HP OpenView
    Network Node Manager.
    ID# $13   Name $12   Set $10   MMLname $4   CatDesc    $11  \nCompDesc $3
    Severity $8   CompID $6   CompType $5   CatID $14\nAlarmNotify $9   AlarmTime$1
    ParentID $2   AlarmReported $7\n$o
```

Tip For more detailed information about configuring HP OpenView, see Appendix A, "HP OpenView Sample SNMP Configuration," in *Cisco Media Gateway Controller Software Release 7 Installation and Configuration Guide.*

Step 14 Verify that SNMP is working by performing the following steps:

a. Begin monitoring an Ethernet interface for SNMP trap traffic by opening a telnet session, logging in to the active Cisco MGC host as root and entering the following UNIX command:

snoop -d *eth_int* **port 162**

Where *eth_int* is the name of the Ethernet interface.

For example, to execute this command on an Ethernet interface called hme1, you would enter the following command:

snoop -d hme1 port 162

b. Open a second telnet session on the active Cisco MGC, start an MML session and enter a command that causes an alarm to be generated. For example, changing the state of a destination causes an alarm to be generated. To take a destination called dpc1 out-of-service, enter the following MML command:

```
set-dest-state:dpc1:OOS
```

Entering a command like this should cause an trap notification to appear in the first telnet session. For example, the following trap information is displayed in the first telnet session when a destination is taken out-of-service and then returned to service:

```
Using device /dev/hme (promiscuous mode)
    va-perch -> nssuramb4.cisco.com UDP D=162 S=46842 LEN=446
    va-perch -> nssuramb4.cisco.com UDP D=162 S=46842 LEN=446
```

If trap information appears in the first telnet session, the procedure is complete.

If nothing appears in the first telnet session, re-enter the **snoop** command for the other Ethernet interface and repeat the above step. If trap information fails to appear in either Ethernet interface, proceed to Step 15.

Step 15 Contact the Cisco TAC for assistance in resolving this problem. Refer to “Obtaining Technical Assistance” section on page xviii for more information on contacting the Cisco TAC.

Sample Configured snmpd.cf File

The following shows a sample snmpd.cnf file.

Note This sample configuration enables both snmpv1 and snmpv2 traps. Therefore, you will see two coldStart traps when the software is initialized—one for version1 and one for version2.

```
# Entry type: sysDescr
# Entry format: octetString
sysDescr  "SNMPv3 agent from Cisco Systems, Inc."

# Entry type: sysObjectID
# Entry format: OID
sysObjectID  transpath

# Entry type: sysLocation
# Entry format: octetString
sysLocation  "Herndon, Virginia"

# Entry type: sysContact
# Entry format: octetString
sysContact  "Cisco Systems, Inc.  +1 703 484 3000"

# Entry type: sysName
# Entry format: octetString
sysName  "NSSU - MGC"

# Entry type: snmpEnableAuthenTraps
# Entry format: integer
snmpEnableAuthenTraps  1


# Entry type: MAX_THREADS
# Entry format: integer
MAX_THREADS  25


# Entry type: MAX_PDU_TIME
# Entry format: integer
```

```
MAX_PDU_TIME  80000

# Entry type: MAX_OUTPUT_WAITING
# Entry format: integer
MAX_OUTPUT_WAITING  65536

# Entry type: MAX_SUBAGENTS
# Entry format: integer
MAX_SUBAGENTS  15

# Entry type: subagent
# Entry format: octetString

#Entry type: snmpCommunityEntry
#Format:  snmpCommunityIndex  (text)
#         snmpCommunityName  (text)
#         snmpCommunitySecurityName  (text)
#         snmpCommunityContextEngineID  (octetString)
#         snmpCommunityContextName  (text)
#         snmpCommunityTransportTag  (text)
#         snmpCommunityStorageType  (nonVolatile, permanent, readOnly)
snmpCommunityEntry  admin mgcusr mgcusr localSnmpID - - nonVolatile
snmpCommunityEntry  readonly public public localSnmpID - - nonVolatile
snmpCommunityEntry  user private private localSnmpID - - nonVolatile

# Entry type:  communityEntry
 # Entry format:  srCommunityAuthSnmpID      (snmpID)
 #                srCommunityName            (textOctetString)
 #                srCommunityGroupName       (textOctetString)
 #                srCommunityContextSnmpID   (snmpID)
 #                srCommunityContextName     (textOctetString)
 #                srCommunityTransportLabel  (textOctetString)
 #                srCommunityMemoryType      (integer)

# Entry type: snmpEngineBoots
# Entry format: integer
snmpEngineBoots  3

#Entry type: usmUserEntry
#Format:  usmUserEngineID  (octetString)
#         usmUserName  (text)
#         usmUserAuthProtocol  (OID)
#         usmUserPrivProtocol  (OID)
#         usmUserStorageType  (nonVolatile, permanent, readOnly)
#         usmTargetTag  (text)
#         AuthKey  (octetString)
#         PrivKey  (octetString)

#Entry type: vacmAccessEntry
#Format:  vacmGroupName  (text)
#         vacmAccessContextPrefix  (text)
#         vacmAccessSecurityModel  (snmpv1, snmpv2c, snmpv2s, usm, http)
#         vacmAccessSecurityLevel  (noAuthNoPriv, authNoPriv, authPriv)
#         vacmAccessContextMatch  (exact, prefix)
#         vacmAccessReadViewName  (text)
#         vacmAccessWriteViewName  (text)
#         vacmAccessNotifyViewName  (text)
#         vacmAccessStorageType  (nonVolatile, permanent, readOnly)
vacmAccessEntry  User - snmpv1 noAuthNoPriv exact All RemoteWrite All \
    nonVolatile
vacmAccessEntry  User - snmpv2c noAuthNoPriv exact All RemoteWrite All \
    nonVolatile
vacmAccessEntry  Guest - snmpv1 noAuthNoPriv exact All - All nonVolatile
vacmAccessEntry  Guest - snmpv2c noAuthNoPriv exact All - All nonVolatile
vacmAccessEntry  SuperUser - snmpv1 noAuthNoPriv exact All Write All \
    nonVolatile
vacmAccessEntry  SuperUser - snmpv2c noAuthNoPriv exact All Write All \
    nonVolatile

#Entry type: vacmSecurityToGroupEntry
#Format:  vacmSecurityModel  (snmpv1, snmpv2c, snmpv2s, usm, http)
#         vacmSecurityName  (text)
#         vacmGroupName  (text)
#         vacmSecurityToGroupStorageType  (nonVolatile, permanent, readOnly)
vacmSecurityToGroupEntry  snmpv1 mgcusr SuperUser nonVolatile
vacmSecurityToGroupEntry  snmpv1 public Guest nonVolatile
vacmSecurityToGroupEntry  snmpv1 private User nonVolatile
vacmSecurityToGroupEntry  snmpv2c mgcusr SuperUser nonVolatile
vacmSecurityToGroupEntry  snmpv2c public Guest nonVolatile
vacmSecurityToGroupEntry  snmpv2c private User nonVolatile

#Entry type: vacmViewTreeFamilyEntry
#Format:  vacmViewTreeFamilyViewName  (text)
#         vacmViewTreeFamilySubtree  (OID)
#         vacmViewTreeFamilyMask  (octetString)
#         vacmViewTreeFamilyType  (included, excluded)
#         vacmViewTreeFamilyStorageType  (nonVolatile, permanent, readOnly)
vacmViewTreeFamilyEntry  All iso - included nonVolatile
vacmViewTreeFamilyEntry  All 0.0 - included nonVolatile
vacmViewTreeFamilyEntry  All hrSWRunEntry.0.2147483647 ff:df excluded \
    nonVolatile
vacmViewTreeFamilyEntry  All hrSWRunPerfEntry.0.2147483647 ff:df excluded \
    nonVolatile
vacmViewTreeFamilyEntry  Write iso - included nonVolatile
vacmViewTreeFamilyEntry  Write mib_2 - excluded nonVolatile
vacmViewTreeFamilyEntry  RemoteWrite iso - included nonVolatile
vacmViewTreeFamilyEntry  RemoteWrite mib_2 - excluded nonVolatile
vacmViewTreeFamilyEntry  RemoteWrite critAppProcEntry.0.1 ff:f7 excluded \
    nonVolatile
vacmViewTreeFamilyEntry  RemoteWrite critAppProcEntry.0.2 ff:f7 excluded \
    nonVolatile
vacmViewTreeFamilyEntry  RemoteWrite critAppProcEntry.0.3 ff:f7 excluded \
    nonVolatile
vacmViewTreeFamilyEntry  RemoteWrite critAppProcEntry.0.4 ff:f7 excluded \
    nonVolatile

#Entry type: snmpNotifyEntry
#Format:  snmpNotifyName  (text)
#         snmpNotifyTag  (text)
#         snmpNotifyType  (trap(1), inform(2))
#         snmpNotifyStorageType  (nonVolatile, permanent, readOnly)
snmpNotifyEntry  32 TrapSink trap nonVolatile

#Entry type: snmpTargetAddrEntry
#Format:  snmpTargetAddrName  (text)
#         snmpTargetAddrTDomain  (snmpUDPDomain, snmpIPXDomain, etc.)
#         snmpTargetAddrTAddress  (transport address,i.e. 192.147.142.254:0)
#         snmpTargetAddrTimeout  (integer)
#         snmpTargetAddrRetryCount  (integer)
#         snmpTargetAddrTagList  (text)
#         snmpTargetAddrParams  (text)
#         snmpTargetAddrStorageType  (nonVolatile, permanent, readOnly)
#         snmpTargetAddrTMask  (transport mask, i.e. 255.255.255.255:0)
#         snmpTargetAddrMMS  (integer)
snmpTargetAddrEntry  34 snmpUDPDomain 127.0.0.1:0 100 3 TrapSink \
    v2cExampleParams nonVolatile 255.255.255.255:0 2048

#Entry type: snmpTargetParamsEntry
```

```
#Format:  snmpTargetParamsName  (text)
#         snmpTargetParamsMPModel  (integer)
#         snmpTargetParamsSecurityModel  (snmpv1, snmpv2c, snmpv2s, usm)
#         snmpTargetParamsSecurityName  (text)
#         snmpTargetParamsSecurityLevel  (noAuthNoPriv,authNoPriv,authPriv)
#         snmpTargetParamsStorageType  (nonVolatile, permanent, readOnly)
snmpTargetParamsEntry  v1ExampleParams 0 snmpv1 public noAuthNoPriv \
    nonVolatile
snmpTargetParamsEntry  v2cExampleParams 1 snmpv2c public noAuthNoPriv \
    nonVolatile

#Entry type: snmpNotifyFilterProfileEntry
#Format:  snmpTargetParamsName  (text)
#         snmpNotifyFilterProfileName  (text)
#         snmpNotifyFilterProfileStorageType  (nonVolatile,permanent,readOnly)

#Entry type: snmpNotifyFilterEntry
#Format:  snmpNotifyFilterProfileName  (text)
#         snmpNotifyFilterSubtree  (OID)
#         snmpNotifyFilterMask  (octetString)
#         snmpNotifyFilterType  (included, excluded)
#         snmpNotifyFilterStorageType  (nonVolatile, permanent, readOnly)

#Entry type: httpUserNameEntry
#Format:  httpUserName  (text)
#         httpUserGroupName  (text)
#         httpUserTransportLabel  (text)
#         httpUserStorageType  (nonVolatile, permanent, readOnly)
#         Password  (octetString)
```

Configuring the Execution Environment

This section provides instructions for configuring the SC host execution environment, and contains the following topics:

- Opening the XECfgParm.dat File, page 7-20
- Configuring Basic System Information, page 7-20
- Specifying IP Addresses, page 7-22
- Configuring Engine Parameters, page 7-24
- Configuring Automatic Congestion Control, page 7-25
- Enabling Call Screening, page 7-27
- Configuring Call Detail Record File Output, page 7-27
- Configuring the System Type, page 7-29
- Configuring the Clearing Location and Default Location Parameters, page 7-30
- Configuring *.GWClearChannelAlgorithm Parameter, page 7-33
- Configuring Switchover, page 7-33
- Initializing the Provisioning Object Manager (POM), page 7-37
- Saving the XECfgParm.dat File, page 7-37

The configuration data file, or XECfgParm.dat file (located in /opt/CiscoMGC/etc), lists all the components in the SC host and defines how it operates. The software automatically migrates your data for the previous release in the XECfgParm.dat file to current Release 7 format. The XECfgParm.dat file contains your execution environment parameters. However, only the default logging levels are migrated for the log priority parameters, including the foverd.logPrio parameter. Therefore, if you have set up specialized logging, you need to reset the parameters after software installation by editing the XECfgParm.dat file.

For more information on the XECfgParm.dat file, including sample files, see the *Cisco Media Gateway Controller Software Release 7 Installation and Configuration Guide*.

You must manually edit the execution environment parameters in the XECfgParm.dat file to initialize and configure the SC host software application.

Caution Do not edit any XECfgParm.dat file parameters not listed below, and remember that all parameters are case-sensitive. Otherwise, your system might not work as intended.

Opening the XECfgParm.dat File

To access and edit the XECfgParm.dat file, complete the following steps:

Note If you have two SC host in a continuous-service configuration, the XECfgParm.dat files will be different for each host.

Step 1 Log in to the SC host as root and change to the /opt/CiscoMGC/etc directory, which contains the XECfgParm.dat file used by your system.

Step 2 Open the XECfgParm.dat file with any text editor, such as vi

Tip Migrated parameters are identified in the XECfgParm.dat file. You should verify these parameters; however, you should concentrate on the new parameters when editing the file.

Configuring Basic System Information

To configure basic system information required for your system to function, modify the following parameters in the first section of the XECfgParm.dat file:

Note If a parameter is identified as migrated, the previously configured value was saved during the upgrade and used in the new XECfgParm.dat file after migration.

Parameter	Modification
*.transpathId	To identify the local SC host host in a continuous-service or high-availability system, enter any one- or two-digit integer. **Note** If you have two SC host hosts in a continuous-service or high-availability system, this number must be different in the XECfgParm.dat file for each host.
*.ownTranspathId	To identify the local SC host host in a continuous-service or high-availability system, enter the same value that you used for *.transpathID. **Note** If you have two SC host hosts in a continuous-service or high-availability system, enter this value in the *.peerTranspathID field in the XECfgParm.dat file on the second host server. If you have a simplex system, leave this field blank.
*.peerTranspathId	To identify the peer SC host host in a continuous-service or high-availability system, enter any one- or two-digit integer. The IDs must be unique in an active and a standby pair. **Note** If you have two SC host hosts in a continuous-service or high-availability system, enter the same value that you used for *.transpathID in the XECfgParm.dat file of the second host server in this field. If you have a simplex system, leave it blank.
*.desiredPlatformState	To determine the desired platform state at initialization, enter one of the following values: • **master**—If you have two (active and standby) SC host hosts, and you are editing the file on the active host • **slave**—If you have two (active and standby) SC host hosts, and you are editing the file on the standby host • **standalone**—If you have a simplex system **Note** If you have two SC host hosts in a continuous-service or high-availability system, make sure that the active SC host is set to **master** and the standby host is set to **slave**.

Parameter	Modification
*.SysCheckpointEnabled	To enable or disable checkpointing, enter one of the following values: • **false**—Disables checkpointing. Calls are not preserved during a switchover, and status messages are not sent to the replicator (default). • **true**—Enables checkpointing. Calls that are in the talking state are preserved and survive a control switchover. All status checkpointing information is sent to the replicator on the active side. **Note** If you have two SC host hosts in a switchover configuration, enter **true**. If you have a standalone configuration, enter **false**.
*.numberOfThreads	To specify the number of threads generated by multithreaded processes such as the engine and the log master, enter one of the following values: • **0**—Single CPU (default) • **1**—Two CPUs • **2**—Four CPUs **Note** If you have a multi-CPU system, the engine.SysGeneratedCode parameter must be left as **true** (the default).
*.stPort	Port number used between peer components or processes. Enter any unused port number greater than 1024; for example, 7000. **Note** If you have two SC host hosts in a continuous-service or high-availability configuration, enter a different number for this value in the XECfgParm.dat file on the secondary host; for example, 7001.
*.OwnClli	Common language location identifier. To initiate circuit query validation if circuit queries are supported, enter an alphanumeric string of as many as 24 characters. Default: TTT-SS-BB-XXX Example: 1-22-33-444

Specifying IP Addresses

To specify IP addresses, modify the following parameters in the first section of the XECfgParm.dat file:

Note If there are two Ethernet interfaces defined on the Cisco MGC, it is mandatory to have these on distinct subnets.

For example, consider the following configuration:

```
*.ipAddrLocalA = 172.22.119.108
*.ipAddrLocalB = 172.22.119.54
```

This is not a valid combination because the Ethernet interfaces are on the same subnet. The following example illustrates a valid combination:

```
*.ipAddrLocalA = 172.22.119.108
*.ipAddrLocalB = 172.22.120.54
```

If the two Ethernet interfaces are on the same subnet, then one of them must be physically disconnected from the existing subnet and then connected to a different subnet. The new IP address must be appropriately configured on the system. Refer to the manual pages for the UNIX command ifconfig for more information.

Parameter	Modification
*.ipAddrLocalA	Enter the first local IP address; used for checkpointing and switchover heartbeats. **Note** This address is the same value as *.IP_Addr1, and is the hme0 interface. ⚠ **Caution** No other machine on the network should have *.ipAddrLocalA set to 0.0.0.0.
*.ipAddrPeerA	Enter the first corresponding peer IP address; used for checkpointing and switchover heartbeats. **Note** If you have two SC host hosts in a continuous-service or high-availability configuration, this value is set to the IP address of the second host.
*.ipAddrLocalB	Enter the second local IP address; used for checkpointing and switchover heartbeats. This is the address of the hme1 interface. **Note** If your configuration does not use a secondary Ethernet adapter, leave this address set to the default value, 0.0.0.0.
*.ipAddrPeerB	Enter the second corresponding peer IP address; used for checkpointing and switchover heartbeats. This is the address of the hme1 interface on the second host. **Note** If your configuration does not use a secondary Ethernet adapter, leave this address set to the default value, 0.0.0.0.
*.IP_Addr1	Enter the IP address of the hme0 interface.
*.IP_Addr2	Enter the IP address of the hme1 interface (if configured).

Parameter	Modification
*.IP_Addr3	Enter the IP address of the hme2 interface (if configured).
*.IP_Addr4	Enter the IP address of the hme3 interface (if configured).

Configuring Engine Parameters

In order for the engine to run correctly, you must modify the following parameters in the Engine section of the XECfgParm.dat file:

Parameter	Modification
engine.CALL_MEM_BLOCK_SIZE	Block of memory allocated per call. Used by MDL. Default: 0 • For memory-critical configurations, use the default value. • For performance-critical configurations, set this value to **110000**.
engine.CALL_MEM_CHUNK_SIZE	Memory chunks allocated from the block of memory designated with engine.CALL_MEM_BLOCK_SIZE. Default: 0 • For memory-critical configurations, use the default value. • For performance-critical configurations, set this value to **110000**.
engine.SysCdrCollection	To designate the format of call detail records (CDRs), enter one of the following values: • **true**—Generates fold-style nontagged CDRs • **false**—Generates new tag, length, and value (TLV) format CDRs (default) **Note** Typically, this value should be **false**.
engine.SysVirtualSwitch	To indicate whether the SC host host functions as a signaling controller or a virtual switch controller, enter one of the following values: • **0**—Signaling controller (nailed trunks, no auditing is initiated) • **1**—Virtual switch controller (switched trunks)
engine.SysGRSTimerInterval	To specify the interval between blocks of Circuit Group Reset (GRS) messages when the engine.SysGRSBlockSize parameter is used, set to the value required (in milliseconds).

Parameter	Modification
engine.SysGRSBlockSize	Many GRS messages can become due for sending at the same time. This situation occurs if you have set the *.GRSEnabled parameter to true during provisioning. The *.GRSEnabled parameter is a property that is set on an SS7 signaling service (in the CMM) or an SS7 path (in MML). GRS messages can be staggered if you send them in blocks. Set the engine.SysGRSBlockSize parameter to the number of messages to be sent in each block. Use the engine.SysGRSTimerInterval parameter to set the time from the start of one block to the start of the next. Default: **0** **Note** This parameter operates independently for each SS7 route (each OPC/DPC pair).
engine.SysGeneratedCode	To determine whether compiled or interpreted code is used, enter one of the following values: • **true**—System uses compiled code (default). • **false**—System uses interpreted code (used only for engineering and debugging). **Note** Compiled code runs faster than interpreted code. Typically, this value should be **true**. If your configuration uses multiple CPUs, this value *must* be **true**.

Configuring Automatic Congestion Control

As of release 7.4(11), the Cisco SC2200 supports Automatic Congestion Control (ACC). ACC regulates traffic to levels that can be handled effectively by the network by rejecting traffic when the system is congested. This increases the throughput of completed calls through the telephone network during periods of overload.

When the Cisco MGC is congested, an Automatic Congestion Level (ACL) indication is sent to adjacent signaling points using SS7 ISUP. Until the congestion abates, a certain percentage of calls are rejected. Detection of congestion is based on the measurement of the Cisco MGC's CPU utilization level.

ACC is controlled by parameters that are found in the XECfgParm.dat file and by a property associated with the signaling service, which are described in the following sections:

- Overload Level Percentage Parameters, page 7-26
- CPU Timer Interval Parameter, page 7-26
- Maximum ACL Value, page 7-26

Overload Level Percentage Parameters

Use the following XECfgParm.dat parameters to set the overload level percentages:

Parameter	Description	Default Value	Valid Range
Ovl1OnsetThresh	Percentage of total CPU utilization at which overload level 1 is reached.	82	0 through 100
Ovl1AbateThresh	Percentage of total CPU utilization at which overload level 1 abates.	75	0 through 100
Ovl1RejectPercent	Percentage of calls that are rejected while overload level 1 is active.	25	0 through 100
Ovl2OnsetThresh	Percentage of total CPU utilization at which overload level 2 is reached.	90	0 through 100
Ovl2AbateThresh	Percentage of total CPU utilization at which overload level 2 abates.	77	0 through 100
Ovl2RejectPercent	Percentage of calls that are rejected while overload level 2 is active.	50	0 through 100
Ovl2OnsetThresh	Percentage of total CPU utilization at which overload level 2 is reached.	93	0 through 100
Ovl2AbateThresh	Percentage of total CPU utilization at which overload level 2 abates.	85	0 through 100
Ovl2RejectPercent	Percentage of calls that are rejected while overload level 2 is active.	100	0 through 100

CPU Timer Interval Parameter

The CPUTimerInterval parameter is used to specify the interval, in milliseconds, at which the CPU utilization level of the Cisco MGC is sampled. The default value is 1000. We recommend that you stay within the range of 500 to 2000 milliseconds.

Maximum ACL Value

Another component in ACC is the maximum ACL value. Since ANSI- and ITU-based signaling points have different maximum ACL values, the Cisco MGC uses a property, MaxACL, associated with an SS7 signaling service or trunk group to map the internal maximum ACL value to the value used by the adjacent signaling point.

When the Cisco MGC is congested, its congestion level can be reported to adjacent signaling points by the ACL value in the release message. ANSI-based signaling points use a range of 0 through 3 to define congestion and ITU-based signaling points use a range of 0 through 2 to define congestion. When MaxACL is set to 3, the internal maximum ACL value is mapped to the ANSI standard (the default value for MaxACL is 3). When MaxACL is set to 2, the internal maximum ACL value is mapped to the ITU standard. MaxACL also has a third possible setting, 0, which disables the sending of ACL indications in the Release message.

The procedure to set this property can be found in the *Cisco MGC Software Release 7 Operations, Maintenance, and Troubleshooting Guide*.

Enabling Call Screening

To initialize the database that stores call screening information, modify the following parameter in the Engine section of the XECfgParm.dat file:

Parameter	Modification
engine.SysScreeningCheck	To enable or disable the A-number and B-number analysis in the call screening database, enter one of the following values: • If you do not have the database environment set with all the required data populated, set this value to **false** (default). • If you have the database and want the system to access it, set this value to **true**.

Configuring Call Detail Record File Output

To configure call detail record (CDR) file output, modify the following parameters in the Data Dumper and Engine sections of the XECfgParm.dat file:

Parameter	Modification
engine.CDRencodingFormat	To specify the call detail record (CDR) file encoding format, enter one of the following values: • **AnsiCDB**—North American (default) • **ItuCDB**—European
engine.CDRtimeStamp	To specify the CDR file time-stamp unit, enter one of the following values: • **S**—Seconds (default). • **M**—Milliseconds; use this parameter if your configuration uses TCAP. **Note** If you use 1110 in the engine.CDRmessageTypes parameter (for TCAP), you *must* specify milliseconds for the CDRtimeStamp value.

Parameter	Modification
engine.CDRmessageTypes	To specify which call detail blocks (CDBs, statistics taken at various points in a call) are recorded during a call, enter one of the two following sets of values (each number represents a point in a call): • **1010, 1020, 1030, 1040, 1050, 1060, 1070, 1080**—Use this value if your CDR files will be read by a measurement server or by another CDR reader. • **1060, 1110**—Use this value if you will use the TLV converter to view CDR files. **1110**—Generates a CDR file containing all CDBs for a call (end of call). If you choose **1110**, you must specify milliseconds in the CDRtimeStamp parameter. **1060**—Required. **1080**—An external value, used for TCAP.
CDRDmpr.CDR	To indicate whether the standard data dumper writes out CDR files, enter one of the following values: • **true**—Standard data dumper opens a CDR file and logs call detail blocks (CDBs). • **false**—Standard data dumper does not open a CDR file and does not log CDBs. **Note** The default CDR file format has been changed from an ASCII format in Release 4 to a binary format in Release 7. Use the dmpr.callDetail parameter to convert the files to an ASCII format, if necessary.
CDRDmpr.callDetail	If your configuration requires ASCII-formatted CDR files, enter **/opt/CiscoMGC/bin/converter**. **Default: /opt/CiscoMGC/local/cdbscript.sh** Use this value if you have created a script to process CDRs; this script is stored as **cdbscript.sh**. **Optional: /opt/CiscoMGC/bin/converter** Use this value if binary CDR files need to be converted to ASCII. For maximum performance, change this value to none, as follows: **cdrDmpr.callDetail = #** **Note** The default CDR file format is binary format. The command above automatically generates CDR files in an ASCII, comma-delimited format in addition to the default, binary format. The ASCII file has a .csv extension. For more information on generating and viewing CDR files, see *Cisco Media Gateway Controller Software Release 7 Operations, Maintenance, and Troubleshooting Guide*.

Note For a detailed description of CDR files, see *Cisco Media Gateway Controller Software Release 7 Billing Interface Guide*.

Configuring the System Type

To configure system alarm information, modify the following parameter in the XE section of the XECfgParm.dat file:

Parameter	Modification
XE.systemType	To specify the system type for alarm LEDs, enter one of the following values: • **NETRA**—Sun Solaris Netra t 1100, t 1120 (internal LEDs, alarm relays) • **SPARC**—Generic box (no alarm relays) • **SPARC-ARU**—Generic box (external alarm relays) Default: SPARC

Configuring the Clearing Location and Default Location Parameters

This property overrides the Clearing Location and Default Location fields in Call Context. Change the clearing location value if you need a value other than the default to be sent to the switch. Change the default location value if you need to define a customer-specific default location for your system that can differ from the default location set in the type definition of the protocol.

Parameter	Modification
ClearingLocation	This property overrides the Clearing Location field in Call Context. Change this value if you need a value other than the default to be sent to the switch. Valid values are: • 0—The Cisco MGC software uses the default Clearing Location in Call Context. • 1—The Cisco MGC software overrides the Clearing Location in Call Context with LOCATION_USER. • 2—The Cisco MGC overrides the Clearing Location in Call Context with LOCATION_ PRIVATE_LOCAL. • 3—The Cisco MGC overrides the Clearing Location in Call Context with LOCATION_ PUBLIC_LOCAL. • 4—The Cisco MGC software overrides the Clearing Location in Call Context with LOCATION_TRANSIT. • 5—The Cisco MGC software overrides the Clearing Location in Call Context with LOCATION_ PUBLIC_REMOTE. • 6—The Cisco MGC overrides the Clearing Location in Call Context with LOCATION_ PRIVATE_REMOTE. • 7—The Cisco MGC overrides the Clearing Location in Call Context with LOCATION_ INTERNATIONAL. • 8—The Cisco MGC overrides the Clearing Location in Call Context with LOCATION_ INTERWORKING. • 9—The Cisco MGC overrides the Clearing Location in Call Context with LOCATION_ LOCAL_INTERFACE. • 10—The Cisco MGC overrides the Clearing Location in Call Context with LOCATION_ LOCAL_LOCAL. • 11—The Cisco MGC overrides the Clearing Location in Call Context with LOCATION_ LOCAL_REMOTE. • 12—The Cisco MGC overrides the Clearing Location in Call Context with LOCATION_ PACKET_MANAGER. • 13—The Cisco MGC overrides the Clearing Location in Call Context with LOCATION_ UNKNOWN.

Parameter	Modification
DefaultLocation	This property overrides the Default Location field in Call Context. Change this value if you need to define a customer-specific default location for your system that can differ from the default location set in the type definition of the protocol. Valid values are: • 0—The Cisco MGC software uses the Default Location in Call Context. • 1—The Cisco MGC software overrides the Default Location in Call Context with LOCATION_USER. • 2—The Cisco MGC software overrides the Default Location in Call Context with LOCATION_PRIVATE_LOCAL. • 3—The Cisco MGC software overrides the Default Location in Call Context with LOCATION_PUBLIC_LOCAL. • 4—The Cisco MGC software overrides the Default Location in Call Context with LOCATION_TRANSIT. • 5—The Cisco MGC software overrides the Default Location in Call Context with LOCATION_PUBLIC_REMOTE. • 6—The Cisco MGC software overrides the Default Location in Call Context with LOCATION_PRIVATE_REMOTE. • 7—The Cisco MGC software overrides the Default Location in Call Context with LOCATION_INTERNATIONAL. • 8—The Cisco MGC software overrides the Default Location in Call Context with LOCATION_INTERWORKING. • 9—The Cisco MGC software overrides the Default Location in Call Context with LOCATION_LOCAL_INTERFACE. • 10—The Cisco MGC software overrides the Default Location in Call Context with LOCATION_LOCAL_LOCAL. • 11—The Cisco MGC software overrides the Default Location in Call Context with LOCATION_LOCAL_REMOTE. • 12—The Cisco MGC software overrides the Default Location in Call Context with LOCATION_PACKET_MANAGER. • 13—The Cisco MGC software overrides the Default Location in Call Context with LOCATION_UNKNOWN.

Configuring *.GWClearChannelAlgorithm Parameter

Clear channel calls get through only if you set the *.GWClearChannelAlgorithm parameter to a value other than null. This parameter is sent to the Cisco MGC when the connection is created and matches the Cisco MGC's clear channel parameter.

Configuring Switchover

To configure switchover, modify the following parameters in the Foverd section of the XECfgParm.dat file:

:

Parameter	Modification
foverd.conn1Type	To set the connection type for connection number 1, enter **serial** or **socket**. **Note** Typically, set this value to **socket**.
foverd.ipLocalPortA	To define the local port number used for IP communication, enter a unique number, keeping the following in mind: • Typically, if Type is socket, set this value to **1051**. • If you have two SC host hosts in a continuous-service or high-availability configuration, enter the foverd.ipLocalPortA value in the foverd.ipPeerPortA field in the XECfgParm.dat file on the secondary host. **Caution** The value of foverd.ipLocalPortA must be unique for every host on the network. Otherwise, active and standby hosts cannot communicate properly. In the instance discussed here, no other machine on the network can have foverd.ipLocalPortA set to 1051. If another machine does have that value, the active and standby hosts cannot perform proper switchover.

Parameter	Modification
foverd.ipPeerPortA	To define the peer port number used for IP communication, enter a unique number, keeping the following in mind: • Typically, if Type is socket, set this value to **1052**. • If you have two SC host hosts in a switchover configuration, enter the foverd.ipPeerPortA value in the foverd.ipLocalPortA field in the XECfgParm.dat file on the secondary host. **Caution** The value of foverd.ipPeerPortA must be unique for every host on the network. Otherwise, active and standby hosts cannot communicate properly. In the instance discussed here, no other machine on the network can have foverd.ipPeerPortA set to 1052. If another machine does have that value, the active and standby hosts cannot perform proper switchover.
foverd.conn2Type	To set the connection type for connection number 2, enter **serial** or **socket**. **Note** Typically, set this value to **socket**.
foverd.ipLocalPortB	To define the secondary local port number used for IP communication, enter a unique number, keeping the following in mind: • Typically, if Type is socket, set this value to **1053**. • If you have two SC host hosts in a switchover configuration, enter this value in the foverd.ipPeerPortB field in the XECfgParm.dat file on the secondary host. **Caution** The value of foverd.ipLocalPortB must be unique for every host on the network. Otherwise, active and standby hosts cannot communicate properly. In the instance discussed here, no other machine on the network can have foverd.ipLocalPortB set to 1053. If another machine does have that value, the active and standby hosts cannot perform proper switchover.

Parameter	Modification
foverd.ipPeerPortA	To define the peer port number used for IP communication, enter a unique number, keeping the following in mind: - Typically, if Type is socket, set this value to **1052**. - If you have two SC host hosts in a switchover configuration, enter the foverd.ipPeerPortA value in the foverd.ipLocalPortA field in the XECfgParm.dat file on the secondary host. **Caution** The value of foverd.ipPeerPortA must be unique for every host on the network. Otherwise, active and standby hosts cannot communicate properly. In the instance discussed here, no other machine on the network can have foverd.ipPeerPortA set to 1052. If another machine does have that value, the active and standby hosts cannot perform proper switchover.
foverd.conn2Type	To set the connection type for connection number 2, enter **serial** or **socket**. **Note** Typically, set this value to **socket**.
foverd.ipLocalPortB	To define the secondary local port number used for IP communication, enter a unique number, keeping the following in mind: - Typically, if Type is socket, set this value to **1053**. - If you have two SC host hosts in a switchover configuration, enter this value in the foverd.ipPeerPortB field in the XECfgParm.dat file on the secondary host. **Caution** The value of foverd.ipLocalPortB must be unique for every host on the network. Otherwise, active and standby hosts cannot communicate properly. In the instance discussed here, no other machine on the network can have foverd.ipLocalPortB set to 1053. If another machine does have that value, the active and standby hosts cannot perform proper switchover.

Parameter	Modification
foverd.ipPeerPortB	To define the secondary local port number used for IP communication, enter a unique number, keeping the following in mind: • Typically, if Type is socket, set this value to **1054**. • If you have two SC host hosts in a switchover configuration, enter this value in the foverd.ipLocalPortB field in the XECfgParm.dat file on the secondary host. **Caution** The value of foverd.ipPeerPortB must be unique for every host on the network. Otherwise, master and slave hosts cannot communicate properly. In the instance discussed here, no other machine on the network can have foverd.ipPeerPortB set to 1054. If another machine does have that value, the master and slave hosts cannot perform proper switchover.
foverd.conn3Type	To set the connection type for connection number 3, enter **serial** or **socket**. **Note** Typically, set this value to **serial**.
foverd.conn3Addr	To specify the address of the peer system, enter a location; for example, /dev/term/a. If your configuration does not use connection number 3, enter **/dev/null** (default). **Note** If your configuration uses an 8-port connector as a serial connection for switchover, you must modify the read-write permissions for the connection. For more information, see *Release Notes for Cisco Media Gateway Controller Software Release 7*.
foverd.abswitchPort	To specify the port used for communication with the A/B switch, enter a location; for example, /dev/term/a. **Note** If your configuration does not use an A/B switch, use the default value (/dev/null).
foverd.heartbeatInterval	Specifies the maximum time in milliseconds between heartbeat messages from the peer switchover daemon. This interval defines the frequency with which the switchover daemon exchanges heartbeat messages with its peer. Default: 4000 milliseconds (4 seconds).

Note For more information on switchover, see the *Cisco Media Gateway Controller Software Release 7 Operations, Maintenance, and Troubleshooting Guide*.

Initializing the Provisioning Object Manager (POM)

To configure the Provisioning Object Manager (POM), modify the following parameters in the POM section of the XECfgParm.dat file:

Parameter	Information	Modification
pom.dataSync	New parameter	Used in a continuous-service configuration to indicate that the POM should synchronize the provisioning data at startup. If you have a standalone system, set this value to **false**. **Note** In the upgrade, if you have a continuous-service or high-availability configuration, you must initially set this value on the second host server you are upgrading to **false**. After you upgrade the second SC host and both hosts are running the same version of software, you must change this value to **true**.
pom.port	New parameter	Used in a continuous-service configuration to indicate the port number the POM uses to communicate with its peer. Enter any integer from **4001** through **4050**, or **default**. **Note** This is a platform-specific value and depends on your system installation. You should only modify this value if the default port (**4001**) is being used by another process or application.

Saving the XECfgParm.dat File

Save your changes and close the editor.

Note For a complete list of parameters, their function, definition, and example values, see the *Cisco Media Gateway Controller Software Release 7 Reference Guide.*

This completes the XE configuration. Continue the upgrade process as described in your chosen upgrade procedure.

Configuring SCP Queries

The Signal Control Point (SCP) translates routing information for the Advanced Intelligent Network (AIN) database queries over TCAP. This section provides instructions for selecting the type of translation you will use to enable SCP database queries. The trigger.dat file (located in /opt/CiscoMGC/etc/trigger.dat), contains the message sending table that contains translation values. You must manually edit the parameters in the trigger.dat file to enable SCP queries.

This section contains the following topics:

- Before You Start, page 7-38
- Configuring the trigger.dat File Attributes, page 7-38

Caution Do not edit any trigger.dat file parameters not listed below, and remember that all parameters are case-sensitive. Otherwise, your system might not work as intended.

For more information on the trigger.dat file, including a sample configured file, see *Cisco Media Gateway Controller Software Release 7 Installation and Configuration Guide.*

Before You Start

You will need to know the translationType value from the Global Title Translation tables on the STP. Get this value from the administrator of your STP.

Configuring the trigger.dat File Attributes

Note The trigger.dat file is not overwritten during software installation. All changes to the trigger.dat file are contained in a file called trigger.template that is installed with the new software. If you modify the trigger.dat file after installing a new software release, you need to view the trigger.template file and copy any changes in that file to your trigger.dat file.

Caution Improper editing of the trigger.dat file can cause service interruption and prevent the Cisco MGC from correctly performing SCP database queries.

You can configure the following Cisco MGC trigger.dat file attributes to perform a Transaction Capabilities Application Part (TCAP) query:

- Global Title Translation
- Service Key Value
- Translation Type

Configuring the Global Title Translation Attribute

Perform the following steps to configure the Global Title Translation attribute:

Step 1 Back up the trigger.dat file.

Step 2 Determine the Trigger Number that you need to edit. You can get this information from your network administrator.

Step 3 Navigate to directory /opt/CiscoMGC/etc.

Step 4 Open the trigger definition file in an ASCII text editor and search for the string *$TriggerTable*.

Step 5 Starting after the $TriggerTable line, count the number of rows equal to the TriggerType beginning from the number 1.

Note Do not count any row that is blank or that begins with a pound sign (#).

Step 6 When you find your row, note down the second number in that row. This number is the index to the $MessageSending table.

Step 7 Edit the file as follows:

a. In the $MessageSending table, select column 9, gtSsn (see Table 7-2).

b. In the table for your translation type, change the Global Title Translation value (column F9) to either 0 or 1. You can get this information from your network administrator. If the number is 0, use GTT. If the number is 1, use PC/SSN.

c. If you change the gtSsn value to 0, you must go to gtFormat in column 16 and reset the value to 0. If you set the value to 1, you must also set column 16 to a non-zero value.

Note See Table 7-2 for table values.

Step 8 Save your changes and close the editor.

Step 9 For your changes to take effect you must reboot the SC host by entering the following command:

```
# /etc/init.d/CiscoMGC start
```

Configuring the Service Key Value Attribute

Perform the following steps to configure the Service Key Value (tcv_sk) attribute:

Step 1 Back up the trigger.dat file.

Step 2 Determine the Trigger Number that you need to edit. You can get this information from your network administrator.

Step 3 Navigate to directory /opt/CiscoMGC/etc.

Step 4 Open the trigger definition file in an ASCII text editor and search for the string *$TriggerTable*.

Step 5 Starting after the $TriggerTable line, count the number of rows equal to the TriggerType beginning from the number 1.

Note Do not count any row that is blank or that begins with a pound sign (#).

Step 6 When you find your row, note down the second number in that row. This number is the index to the $MessageSending table.

Caution **Do not change TCVs**. You must verify that column 2 is equal to 1 before changing tcv_sk. If column 2 is not equal to 1, this is not an ETSI trigger and column 6 is a TCV, not an SK.

Step 7 Edit the file as follows:

a. In the $MessageSending table, select tcv_sk, in column 6 (see Table 7-2).

b. In the table, change the value for tcv_sk to a value from 0 through 255. You can get this information from your network administrator.

Step 8 Save your changes and close the editor.

Step 9 Restart the SC host software by entering the following command:

```
# /etc/init.d/CiscoMGC start
```

Configuring the Translation Type Attribute

Perform the following steps to configure the Translation Type (translationType) attribute:

Step 1 Back up the trigger.dat file.

Step 2 Determine the Trigger Number that you need to edit. You can get this information from your network administrator.

Step 3 Navigate to directory /opt/CiscoMGC/etc.

Step 4 Open the trigger definition file in an ASCII text editor and search for the string *$TriggerTable*.

Step 5 Starting after the $TriggerTable line, count the number of rows equal to the TriggerType beginning from the number 1.

Note Do not count any row that is blank or that begins with a pound sign (#).

Step 6 When you find your row, note down the second number in that row. This number is the index to the $MessageSending table.

Caution You must verify that column 2 is equal to 2 or 3 before changing Translation Type. If column 2 is not equal to 2 or 3, this is not an ANSI trigger and Translation Type is not used.

Step 7 Edit the file as follows:

a. In the $MessageSending table, select translationType, in column 7 (see Table 7-2).

b. In the table for your translation type, change the value for translationType to a value from 0 through 255. You can get this information from your network administrator.

Step 8 Save your changes and close the editor.

Step 9 For your changes to take effect you must reboot the SC host by entering the following command:

```
# /etc/init.d/CiscoMGC start
```

Table 7-2 $MessageSending Table Values

F1	F2	F3	F4	F5	F6	F7	F8	F9	F10	F11	F12	F13	F14	F15	F16	F17	F18	F19	F20	F21
Transport	**tcapType**	**stpScpGroupIndex**	**msg**	**asn1Encoding**	**tcv_sk**	**translationType**	**tcapBodyType**	**gtSsn**	**dpcPres**	**ssnPres**	**dpcNetwork**	**dpcCluster**	**dpcMember**	**ssn**	**gtFormat**	**OS1**	**OS2**	**OS3**	**OS4**	**OS5**
# MS 1: xxxxxx LNP																				
1	2	0	6	0	0	255	1	0	0	1	0	0	0	0	2	1	0	0	0	0
# MS 2: Generic LNP																				
1	2	0	6	0	37	255	1	0	0	1	0	0	0	0	2	2	0	0	0	0
# MS 3: xxxxxxx 800																				
2	1	1	1	0	0	0	1	0	0	1	0	0	0	0	2	3	0	0	0	0
# MS 4: ANSI AIN 800 NPA																				
1	2	0	6	0	4	255	1	0	0	1	0	0	0	0	2	4	0	0	0	0
# MS 5: ANSI AIN 800 NPA-NXX																				
1	2	0	6	0	5	255	1	0	0	1	0	0	0	0	2	4	0	0	0	0
# MS 6: ANSI AIN 800 NPA-NXX-XXX																				
1	2	0	6	0	8	255	1	0	0	1	0	0	0	0	2	4	0	0	0	0
# MS 7: ANSI AIN 800 Termination information																				
1	2	0	5	0	0	255	1	0	0	1	0	0	0	0	2	5	0	0	0	0
# MS 8: ANSI PRE AIN 800																				
1	3	0	6	0	0	254	2	0	0	1	0	0	0	0	2	6	0	0	0	0
# MS 9: ANSI PRE AIN 800 Termination information																				
1	3	0	5	0	0	254	2	0	0	1	0	0	0	0	2	7	0	0	0	0

Sample trigger.dat File

```
#--//****************************************************************************
#--//* Table_9.trigger                                                          *
#--//*                                                                          *
#--//* TRIGGER TABLES                                                           *
#--//*                                                                          *
#--//* (c) 1999-2000 CISCO SYSTEMS, INC..  ALL RIGHTS RESERVED.                 *
#--//* THIS SOFTWARE CONTAINS CONFIDENTIAL INFORMATION AND TRADE SECRETS OF      *
#--//* CISCO SYSTEMS, INC..  USE, DISCLOSURE, OR REPRODUCTION IS PROHIBITED      *
#--//* WITHOUT THE PRIOR EXPRESS WRITTEN PERMISSION OF THE CISCO SYSTEMS, INC..  *
#--//*                                                                          *
#--//****************************************************************************
# "$Id: Table_9.trigger,v 1.11.2.3 1999/09/20 18:20:51 xxxxxxxx Exp $";
# "(c) 1999-2000 Cisco Systems, Inc..  All Rights Reserved."
```

```
#############
$TriggerTable
#############
# All fields are pointers to records of other types
# F1   F2   F3   F4   F5   F6   F7
# MA   MS   RR1  RR2  RR3  RR4  RR5

#----------------------------------
# TT 1: xxxxxx LNP
#----------------------------------
  1    1    1    2    0    0    0

#----------------------------------
# TT 2: Generic LNP
#----------------------------------
  2    2    1    3    0    0    0

#----------------------------------
# TT 3: xxxxxxx 800
#----------------------------------
  3    3    10   4    5    0    0

#----------------------------------
# TT 4: ANSI AIN 800 NPA
#----------------------------------
  4    4    10   6    7    0    0

#----------------------------------
# TT 5: ANSI AIN 800 NPA-NXX
#----------------------------------
  4    5    10   6    7    0    0

#----------------------------------
# TT 6: ANSI AIN 800 NPA-NXX-XXXX
#----------------------------------
  4    6    10   6    7    0    0

#----------------------------------
# TT 7: ANSI AIN 800 Termination Information
#----------------------------------
  5    7    10   0    0    0    0

#----------------------------------
# TT 8: ANSI PRE AIN AIN 800
#----------------------------------
  4    8    10   8    9    0    0

#----------------------------------
# TT 9: ANSI PRE AIN 800 Termination Information
#----------------------------------
  5    9    10   0    0    0    0


##############
$MessageAction
##############
#
# F1   F2   F3   F4   F5   F6   F7   F8   F9   F10
# ACT1 REQ  ACT2 REQ  ACT3 REQ  ACT4 REQ  ACT5 REQ

#-------------------------------------------------
# MA 1: xxxxxx LNP
```

```
#-------------------------------------------------
  1    1    3    0    0    0    0    0    0    0

#-------------------------------------------------
# MA 2: Generic LNP
#-------------------------------------------------
  1    1    2    1    3    0    0    0    0    0

#-------------------------------------------------
# MA 3: xxxxxxx 800
#-------------------------------------------------
  1    1    3    0    0    0    0    0    0    0

#-------------------------------------------------
# MA 4: ANSI AIN 800 / ANSI PRE AIN 800
#-------------------------------------------------
  1    1    3    0    0    0    0    0    0    0

#-------------------------------------------------
# MA 5: ANSI AIN 800 Termination Information / PRE AIN 800 Termination Information
#-------------------------------------------------
  4    1    0    0    0    0    0    0    0    0


###############
$MessageSending
###############
#
# gtFormat Values
# GTFORMAT_DO_NOT_USE_GLOBAL_TITLE                 := 0
# GTFORMAT_USE_GLOBAL_TITLE_TRANSLATION_TYPE_NUMBERING_SCHEME_ENCODING_SCHEME := 1
# GTFORMAT_USE_GLOBAL_TITLE_TRANSLATION_TYPE       := 2
# GTFORMAT_USE_GLOBAL_TITLE_ONLY                   := 3
# GTFORMAT_UNKNOWN                                 := 4
#
```

Note To see proper formatting for the table below, see Table 7-2.

```
# F1 F2 F3 F4 F5 F6 F7 F8 F9 F10 F11 F12 F13 F14 F15 F16 F17 F18 F19 F20 F21
# transport tcapType stpScpGroupIndex msg asn1Encoding tcv_sk translationType tcapBodyType
gtSsn dpcPres ssnPres dpcNetwork dpcCluster dpcMember ssn gtFormat OS1 OS2 OS3 OS4 OS5

#----------------------------------------------------------------------------------------
# MS 1: xxxxxx LNP
#----------------------------------------------------------------------------------------
1 2 0 6 0 0 255 1 0 0 1 0 0 0 0 2 1 0 0 0 0

#----------------------------------------------------------------------------------------
# MS 2: Generic LNP
#----------------------------------------------------------------------------------------
1 2 6 37 255 0 1 0 0 2 0 0 0 0

#----------------------------------------------------------------------------------------
# MS 3: xxxxxxx 800
#----------------------------------------------------------------------------------------
2 1 1 0 1 0 0 0 2 0 0

#----------------------------------------------------------------------------------------
# MS 4: ANSI AIN 800 NPA
#----------------------------------------------------------------------------------------
1 2 0 6 0 4 255 1 0 0 1 0 0 0 0 2 4 0 0 0 0
```

```
#----------------------------------------------------------------------------------------
# MS 5: ANSI AIN 800 NPA-NXX
#----------------------------------------------------------------------------------------
1 2 0 0 255 0 1 0 0 4 0 0

#----------------------------------------------------------------------------------------
# MS 6: ANSI AIN 800 NPA-NXX-XXX
#----------------------------------------------------------------------------------------
1 2 0 6 0 8 255 1 0 0 1 0 0 0 0 2 4 0 0 0 0

#----------------------------------------------------------------------------------------
# MS 7: ANSI AIN 800 Termination information
#----------------------------------------------------------------------------------------
1 2 0 5 0 0 255 1 0 0 1 0 0 0 0 2 5 0 0 0 0

#----------------------------------------------------------------------------------------
# MS 8: ANSI PRE AIN 800
#----------------------------------------------------------------------------------------
1 3 0 6 0 0 254 2 0 0 1 0 0 0 0 2 6 0 0 0 0

#----------------------------------------------------------------------------------------
# MS 9: ANSI PRE AIN 800 Termination information
#----------------------------------------------------------------------------------------
1 3 0 5 0 0 254 2 0 0 1 0 0 0 0 2 7 0 0 0 0

################
$OperationSending
#################
#
# F1            F2            F3            F4              F5
# componentType opClass       opCodeFamily  opCodeSpecifier opCodeFlag
# F6                   F7
# correlationRequired  PS

#----------------------------------------------------------------------------------------
# OS 1: xxxxxx LNP
#----------------------------------------------------------------------------------------
6 1 3 0

#----------------------------------------------------------------------------------------
# OS 2: Generic LNP
#----------------------------------------------------------------------------------------
6 100 4 2

#----------------------------------------------------------------------------------------
# OS 3: xxxxxxx 800
#----------------------------------------------------------------------------------------
1 0 4 3

#----------------------------------------------------------------------------------------
# OS 4: ANSI AIN 800
#----------------------------------------------------------------------------------------
6 100 4 0 4

#----------------------------------------------------------------------------------------
# OS 5: ANSI AIN 800 Termination Information Should have correlationRequired = 1
#----------------------------------------------------------------------------------------
6 1 103 4 4 0 5

#----------------------------------------------------------------------------------------
# OS 6: ANSI PRE AIN 800
#----------------------------------------------------------------------------------------
6 1 3 1 3 0 6
```

```
#-----------------------------------------------------------------------------------------
# OS 7: ANSI PRE AIN 800 Termination Information
#-----------------------------------------------------------------------------------------
2 1 0 0 0 0 7


################
$ParameterSending
#################
#
# F1   F2   F3   F4   F5   F6   F7   F8   F9   F10  F11  F12  F13  F14  F15  F16  F17 F18
# PA1  REQ  PA2  REQ  PA3  REQ  PA4  REQ  PA5  REQ  PA6  REQ  PA7  REQ  PA8  REQ  PA9 REQ
# F19  F20
# PA10 REQ

#-----------------------------------------------------------------------------------------
# PS 1: xxxxxx LNP
#-----------------------------------------------------------------------------------------
100 1 101 1 102 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0

#-----------------------------------------------------------------------------------------
# PS 2: Generic LNP
#-----------------------------------------------------------------------------------------
100 1 101 1 102 1 103 1 0 0 0 0 0 0 0 0 0 0 0 0

#-----------------------------------------------------------------------------------------
# PS 3: xxxxxxx 800
#-----------------------------------------------------------------------------------------
200 1 201 1 202 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0

#-----------------------------------------------------------------------------------------
# PS 4: ANSI AIN 800 (All types)
#-----------------------------------------------------------------------------------------
100 1 101 1 102 1 103 1 104 1 109 0 110 0 111 0 112 0 113 0

#-----------------------------------------------------------------------------------------
# PS 5: ANSI AIN 800 Termination Information
#-----------------------------------------------------------------------------------------
105 1 106 1 107 0 108 0 0 0 0 0 0 0 0 0 0 0 0 0

#-----------------------------------------------------------------------------------------
# PS 6: ANSI PRE AIN 800
#-----------------------------------------------------------------------------------------
17 1 2 1 16 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0

#-----------------------------------------------------------------------------------------
# PS 7: ANSI PRE AIN 800 Termination Information
#-----------------------------------------------------------------------------------------
21 1 20 1 22 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0


#################
$ReceivedResponse
#################
#
# F1   F2
# MR   RA

#-----------------------------------------------------------------------------------------
# RR 1: xxxxxx LNP / Generic LNP Default
#-----------------------------------------------------------------------------------------
0    1

#-----------------------------------------------------------------------------------------
```

```
# RR 2: xxxxxx LNP 1st expected
#----------------------------------------------------------------------------------------
1    2

#----------------------------------------------------------------------------------------
# RR 3: Generic LNP 1st expected
#----------------------------------------------------------------------------------------
1    3

#----------------------------------------------------------------------------------------
# RR 4: xxxxxxx 800 1st expected (Result)
#----------------------------------------------------------------------------------------
2    1

#----------------------------------------------------------------------------------------
# RR 5: xxxxxxx 800 2st expected (Error)
#----------------------------------------------------------------------------------------
3    4

#----------------------------------------------------------------------------------------
# RR 6: ANSI AIN 800 With termination status notification
#----------------------------------------------------------------------------------------
4    5

#----------------------------------------------------------------------------------------
# RR 7: ANSI AIN 800
#----------------------------------------------------------------------------------------
5    6

#----------------------------------------------------------------------------------------
# RR 8: ANSI PRE AIN 800 With termination status notification
#----------------------------------------------------------------------------------------
6    7

#----------------------------------------------------------------------------------------
# RR 9: ANSI PRE AIN 800
#----------------------------------------------------------------------------------------
7    8

#----------------------------------------------------------------------------------------
# RR 10: ANSI AIN 800 / PRE AIN 800 Default
#----------------------------------------------------------------------------------------
0    9


#################
$MessageReceiving
#################
#
# F1   F2   F3   F4   F5   F6   F7   F8   F9   F10  F11
# MSG  OR1  REQ  OR2  REQ  OR3  REQ  OR4  REQ  OR5  REQ

#------------------------------------------------------
# MR 1: xxxxxx LNP / Generic LNP
#------------------------------------------------------
  8    1    1    0    0    0    0    0    0    0    0

#------------------------------------------------------
# MR 2: xxxxxxx 800 (Result)
#------------------------------------------------------
  3    2    1    0    0    0    0    0    0    0    0

#------------------------------------------------------
# MR 3: xxxxxxx 800 (Error)
```

```
#------------------------------------------------------
  3    3    1    0    0    0    0    0    0    0    0

#------------------------------------------------------
# MR 4: ANSI AIN 800 with termination status notification
#------------------------------------------------------
  8    4    1    5    1    0    0    0    0    0    0

#------------------------------------------------------
# MR 5: ANSI AIN 800
#------------------------------------------------------
  8    4    1    0    0    0    0    0    0    0    0

#------------------------------------------------------
# MR 6: ANSI PRE AIN 800 with termination status notification
#------------------------------------------------------
  8    6    1    7    1    0    0    0    0    0    0

#------------------------------------------------------
# MR 7: ANSI PRE AIN 800
#------------------------------------------------------
  8    6    1    0    0    0    0    0    0    0    0


###################
$OperationReceiving
###################
#
# F1            F2           F3              F4           F5          F6
# componentType opClass      opCodeFamily opCodeSpecifier opCodeFlag PR

#----------------------------------------------------------------------
# OR 1: xxxxxx LNP / Generic LNP
#----------------------------------------------------------------------
  6             1            101          1               4          1

#----------------------------------------------------------------------
# OR 2: xxxxxxx 800 (Result)
#----------------------------------------------------------------------
  1             1            0            20              4          2

#----------------------------------------------------------------------
# OR 3: xxxxxxx 800 (Error)
#----------------------------------------------------------------------
  3             1            0            0               4          3

#----------------------------------------------------------------------
# OR 4: ANSI AIN 800
#----------------------------------------------------------------------
  6             1            101          1               4          4

#----------------------------------------------------------------------
# OR 5: ANSI AIN 800 Request for status notification
#----------------------------------------------------------------------
  6             1            103          5               4          5

#----------------------------------------------------------------------
# OR 6: ANSI PRE AIN 800
#----------------------------------------------------------------------
  6             1            4            1               3          6

#----------------------------------------------------------------------
# OR 7: ANSI PRE AIN 800 Request for status notification
#----------------------------------------------------------------------
```

```
  6             1            6            1               4          7


###################
$ParameterReceiving
###################

# F1   F2   F3   F4   F5   F6   F7   F8   F9   F10  F11  F12  F13  F14  F15  F16
# PA1  REQ  ACT  PA2  REQ  ACT  PA3  REQ  ACT  PA4  REQ  ACT  PA5  REQ  ACT  PA6
  REQ  F17  F18  F19  F20  F21  F22  F23  F24  F25  F26  F27  F28  F29  F30
  ACT  PA7  REQ  ACT  PA8  REQ  ACT  PA9  REQ  ACT  PA10 REQ  ACT

#-----------------------------------------------------------------------------------------
# PR 1: xxxxxx LNP / Generic LNP
#-----------------------------------------------------------------------------------------
102  1    1    0    0    0    0    0    0    0    0    0    0    0    0    0    0    0
0    0    0    0    0    0    0    0    0    0    0    0

#-----------------------------------------------------------------------------------------
# PR 2: xxxxxxx 800 (Result)
#-----------------------------------------------------------------------------------------
205  1    1    206  1    1    204  1    3    0    0    0    0    0    0    0    0    0
0    0    0    0    0    0    0    0    0    0    0    0

#-----------------------------------------------------------------------------------------
# PR 3: xxxxxxx 800 (Error)
#-----------------------------------------------------------------------------------------
205  1    1    206  1    1    204  1    3    0    0    0    0    0    0    0    0    0
0    0    0    0    0    0    0    0    0    0    0    0

#-----------------------------------------------------------------------------------------
# PR 4: ANSI AIN 800 Result
#-----------------------------------------------------------------------------------------
102  1    1    110  0    2    113  0    2    114  1    2    115  1    2    0    0    0
0    0    0    0    0    0    0    0    0    0    0    0

#-----------------------------------------------------------------------------------------
# PR 5: ANSI AIN 800 Status request
#------------------------------------------------------------------------------------------
------------------------------------------------------------
105  1    4    0    0    0    0    0    0    0    0    0    0    0    0    0    0    0
0    0    0    0    0    0    0    0    0    0    0    0

#------------------------------------------------------------------------------------------
------------------------------------------------------------
# PR 6: ANSI PRE AIN 800 Result
#------------------------------------------------------------------------------------------
------------------------------------------------------------
8    0    2    4    1    1    18   0    2    0    0    0    0    0    0    0    0    0
0    0    0    0    0    0    0    0    0    0    0    0

#-----------------------------------------------------------------------------------------
# PR 7: ANSI PRE AIN 800 Status request
#-----------------------------------------------------------------------------------------
20   1    4    0    0    0    0    0    0    0    0    0    0    0    0    0    0    0
0    0    0    0    0    0    0    0    0    0    0    0
```

```
###############
$ResponseAction
###############
#
# F1   F2   F3   F4   F5   F6   F7   F8   F9   F10  F11  F12  F13  F14  F15
# ACT1 REQ  DAT  ACT2 REQ  DAT  ACT3 REQ  DAT  ACT4 REQ  DAT  ACT5 REQ  DAT

#---------------------------------------------------------------------------
# RA 1: xxxxxx LNP Default & Generic LNP Default
#---------------------------------------------------------------------------
  4    1    2    0    0    0    0    0    0    0    0    0    0    0    0

#---------------------------------------------------------------------------
# RA 2: xxxxxx LNP 1st Expected
#---------------------------------------------------------------------------
  4    1    2    0    0    0    0    0    0    0    0    0    0    0    0

#---------------------------------------------------------------------------
# RA 3: Generic LNP 1st Expected
#---------------------------------------------------------------------------
  1    1    0    4    1    2    0    0    0    0    0    0    0    0    0

#---------------------------------------------------------------------------
# RA 4: xxxxxxx (Error)
#---------------------------------------------------------------------------
  0    0    0    0    0    0    0    0    0    0    0    0    0    0    0

#---------------------------------------------------------------------------
# RA 5: ANSI AIN 800 with termination status notification
#---------------------------------------------------------------------------
  2    0    1    4    1    3    0    0    0    0    0    0    0    0    0

#---------------------------------------------------------------------------
# RA 6: ANSI AIN AIN 800
#---------------------------------------------------------------------------
  4    1    3    0    0    0    0    0    0    0    0    0    0    0    0

#---------------------------------------------------------------------------
# RA 7: ANSI PRE AIN 800 with termination status notification
#---------------------------------------------------------------------------
  2    0    4    4    1    3    0    0    0    0    0    0    0    0    0

#---------------------------------------------------------------------------
# RA 8: ANSI PRE AIN 800
#---------------------------------------------------------------------------
  4    1    3    0    0    0    0    0    0    0    0    0    0    0    0

#---------------------------------------------------------------------------
# RA 9: 800 Default
#---------------------------------------------------------------------------
  4    1    3    0    0    0    0    0    0    0    0    0    0    0    0

###########
$ActionData
###########
#
# F1   F2   F3   F4   F5
#-----------------------

# AD 1: ANSI AIN 800  Data for RESULT_ACTION_RE_TRIGGER_VIA_LCM (to send termination
information)
# Trg  Pic   Null Null Null
#--------------------------
  7    13    0    0    0
```

```
# AD 2: ANSI LNP Data for RESULT_ACTION_SEND_ACTION_TO_LCM
# Act  Null Null Null  NULL
#--------------------------
  1    0     0    0    0

# AD 3: ANSI AIN / PRE AIN 800 Data for RESULT_ACTION_SEND_ACTION_TO_LCM
# Act  Null Null Null  NULL
#--------------------------
  2    0     0    0    0

# AD 4: ANSI PRE AIN 800  Data for RESULT_ACTION_RE_TRIGGER_VIA_LCM (to send termination
information)
# Trg  Pic   Null Null Null
#--------------------------
  9    13    0    0    0
```

This completes the SCP configuration. Continue to the next section to initialize the call-screening database. If you have questions or need assistance, see the "Obtaining Technical Assistance" section on page xviii.

Initializing the Call Screening Database

During installation, the installation script (**install.sh**) installs and initializes a database that the SC host can use to store call screening information for number analysis.

You might want to perform white and black list screening to include or exclude calls from certain numbers. You can provision white lists that specify allowed A-numbers (calling numbers) or B-numbers (called numbers). Black lists block specified A-numbers (calling numbers) or B-numbers (called numbers).

The call screening database is stored in the /opt/TimesTen32/datastore directory. The database name is howdydb. The maximum database size, 256 MB, is specified in the .odbc.ini file shown in the ".odbc.ini File Information" section on page 7-50.

This section contains the following topics:

- .odbc.ini File Information, page 7-50
- Setting Up Replication, page 7-51
- Troubleshooting, page 7-55

Note You cannot change the database name.

.odbc.ini File Information

The .odbc.ini file specifies the location of the database storage, and it is located in the /opt/CiscoMGC/local directory.

Following is an example of an .odbc.ini file.

```
[ODBC Data Sources]
howdydb=TimesTen 3.2 Driver
```

```
[howdydb]
Driver=/opt/TimesTen32/32/lib/libtten.so
DataStore= /opt/TimesTen32/datastore/howdydb
DurableCommits=0
ExclAccess=0
ThreadSafe=1
WaitForConnect=0
Size=256

[ODBC]
Trace=0
TraceFile=
Installdir=/opt/TimesTen32/32
```

Setting Up Replication

If you have two telephony controller hosts in a continuous-service or high-availability system, you must set up database replication between the two hosts. During replication, any updates applied to the database on one host are replicated in the database on the other. Data is transferred real time and does not require the committing or deploying of a configuration.

Replication copies data changes to either database after the initial setup. However, if you have data on one host, and you want the same data on another host, you must back up and move the data over, in addition to configuring replication.

If this is the initial installation of the software, and you do not have any data in the database, perform the following steps. If you do have data in one database and want to copy it to the other host, proceed to the "Initializing Replication and Copying the Database to Another Host" section on page 7-52.

Note Before you can initialize the databases, you must install the SC software on both machines.

If you have data in both databases, and the databases do not match, contact the TAC for assistance in merging the databases.

Initializing Database Replication

To set up the initial replication, perform the following steps:

Step 1 Log in to the active host as the root user and enter the following command:

```
setup_replication.sh standbyhost howdydb
```

Where *standbyhost* is the name (not IP address) of your standby host. In Example 7-1, the active host is hostx and the standby host is hosty.

Caution Do not use IP addresses when setting up database replication. If you do, replication fails.

Example 7-1 Initializing Database Replication on the Active Host

```
hostx% setup_replication.sh hosty howdydb

   Setting up replication to node hosty for DSN howdydb
   Adding cisco.whitelist_a
   Adding cisco.blacklist_a
   Adding cisco.whitelist_b
   Adding cisco.blacklist_b
   Adding cisco.portednumbers
   Adding cisco.numberterm
RAM Residence Policy            : inUse
RAM Residence Grace (Secs)      : 0
Manually Loaded In Ram          : False
Purge Logs for Data Store       : True
Logging Enabled                 : True
Replication Manually Started    : True
```

Step 2 Log in to the standby host as the root user and enter the following command:

setup_replication.sh *activehost* **howdydb**

Where *activehost* is the name (not IP address) of your active host. In the Example 7-2, the active host is hostx and the standby host is hosty.

Caution Do not use IP addresses when setting up database replication. If you do, replication fails.

Example 7-2 Initializing Database Replication on the Standby Host

```
hosty% setup_replication.sh hostx howdydb

   Setting up replication to node hostx for DSN howdydb
   Adding cisco.whitelist_a
   Adding cisco.blacklist_a
   Adding cisco.whitelist_b
   Adding cisco.blacklist_b
   Adding cisco.portednumbers
   Adding cisco.numberterm
RAM Residence Policy            : inUse
RAM Residence Grace (Secs)      : 0
Manually Loaded In Ram          : False
Purge Logs for Data Store       : True
Logging Enabled                 : True
Replication Manually Started    : True
```

Proceed to the “Verifying Database Replication” section on page 7-54.

Initializing Replication and Copying the Database to Another Host

If you have existing data in one database and want to copy the data to another machine—for example, from the active to standby machine—perform the following steps:

Step 1 Log in to the active host as the root user and enter the following command:

setup_replication.sh *standbyhost* **howdydb**

Where *standbyhost* is the name (not IP address) of your standby host. In Example 7-3, the active host is hostx and the standby host is hosty.

Caution Do not use IP addresses when setting up database replication. If you do, replication fails.

Example 7-3 Initializing Database Replication on the Active Host

```
hostx% setup_replication.sh hosty howdydb

   Setting up replication to node hosty for DSN howdydb
   Adding cisco.whitelist_a
   Adding cisco.blacklist_a
   Adding cisco.whitelist_b
   Adding cisco.blacklist_b
   Adding cisco.portednumbers
   Adding cisco.numberterm
RAM Residence Policy            : inUse
RAM Residence Grace (Secs)      : 0
Manually Loaded In Ram          : False
Purge Logs for Data Store       : True
Logging Enabled                 : True
Replication Manually Started    : True
```

Step 2 Create a directory for the database backup files using the **mkdir** command. For example:

```
mkdir /backupdb
```

Step 3 Create the backup files by entering the following command:

```
ttRepAdmin -dsn howdydb -receiver -name standbyhost -backup dirname
```

Where *standbyhost* is the name (not IP address) of the standby host and *dirname* is the name of the directory you created in Step 2.

For example:

```
ttRepAdmin -dsn howdydb -receiver -name hosty -backup backupdb
```

Step 4 Transfer the backup files from the active host to the standby host (for example, use FTP to transfer the directory).

Step 5 Log in to the standby host as the root user and destroy the database that has been created during the initial setup of replication. Enter the following command:

```
ttDestroy /opt/TimesTen32/datastore/howdydb
```

Step 6 Restore using the backed-up files from the active host that you transferred. Enter the following command:

```
ttRestore -fname replica -dir dirname DSN=howdydb
```

where *dirname* is the name of the directory you created. For example:

```
ttRestore -fname replica -dir backupdb DSN=howdydb
The restore process is being initiated
Restore complete
```

Step 7 To set up replication of the standby host, enter the following commands:

```
ttRepAdmin -dsn howdydb -self -restored dirname
ttRepAdmin -dsn howdydb -self -swap standbyhost
```

For example:

```
hosty% ttRepAdmin -dsn howdydb -self -restored backupdb
hosty% ttRepAdmin -dsn howdydb -self -swap hosty
Self swap with peer hosty successful
```

Step 8 Enter the following commands to complete the restoration:

```
ttRepAdmin -dsn howdydb -table cisco.whitelist_a -sendto activehost
ttRepAdmin -dsn howdydb -table cisco.whitelist_b -sendto activehost
ttRepAdmin -dsn howdydb -table cisco.blacklist_b -sendto activehost
ttRepAdmin -dsn howdydb -table cisco.blacklist_a -sendto activehost
ttAdmin -repPolicy manual howdydb
ttAdmin -repStart howdydb
```

For example:

```
hosty% ttRepAdmin -dsn howdydb -table cisco.whitelist_a -sendto hostx
hosty% ttRepAdmin -dsn howdydb -table cisco.whitelist_b -sendto hostx
hosty% ttRepAdmin -dsn howdydb -table cisco.blacklist_b -sendto hostx
hosty% ttRepAdmin -dsn howdydb -table cisco.blacklist_a -sendto hostx
hosty% ttAdmin -repPolicy manual howdydb
RAM Residence Policy            : inUse
RAM Residence Grace (Secs)      : 0
Manually Loaded In Ram          : False
Purge Logs for Data Store       : True
Logging Enabled                 : True
Replication Manually Started    : False
hosty% ttAdmin -repStart howdydb
RAM Residence Policy            : inUse
RAM Residence Grace (Secs)      : 0
Manually Loaded In Ram          : False
Purge Logs for Data Store       : True
Logging Enabled                 : True
Replication Manually Started    : True
```

Step 9 Verify the database replication is working. See the "Verifying Database Replication" section on page 7-54.

Verifying Database Replication

To verify that replication is working, perform the following steps:

Step 1 Log in to the active host and start an MML session by entering **mml**.

Step 2 Enter the **prov-sta** MML command to begin a provisioning session. For example:

```
hostx mml> prov-sta::srcver="new",dstver="test",confirm
   VSC-01 - Media Gateway Controller 2000-08-30 11:31:15
M  COMPLD
   "PROV-STA"
   ;
```

Step 3 Add an entry into the B white list database using the **numan-add** MML command. For example:

```
hostx mml> numan-add:bwhite:custgrpid="S018",svcname="testsvc",cli="9998"
   VSC-01 - Media Gateway Controller 2000-08-30 11:31:25
M  COMPLD
   "bwhite"
   ;
```

Step 4 Enter the **prov-stp** MML command to end the provisioning session.

Step 5 Log in to the standby host and start an MML session by entering **mml**.

Step 6 Enter the **prov-sta** MML command to begin a provisioning session. For example:

```
hosty mml>  prov-sta::srcver="new",dstver="test",confirm
```

Step 7 Enter the **numan-rtrv** MML command to verify that the entry you added in Step 3 was replicated to the database on the standby host. For example:

```
hosty mml> numan-rtrv:bwhite:custgrpid="S018",svcname="testsvc",cli="9998"
   VSC-01 - Media Gateway Controller 2000-08-30 11:33:52
M  RTRV
   "session=test:bwhite"
   /* The cli :9998: exists.   */
   ;
```

Step 8 Enter the **prov-stp** MML command to end the provisioning session.

Troubleshooting

If you have problems during replication, try stopping and restarting the replication as follows:

Step 1 Stop the replication by entering:

```
# /etc/init.d/ttreplic stop
```

Step 2 Restart the replication by entering:

```
# /etc/init.d/ttreplic start
```

If you still have problems, retry the commands listed in the "Verifying Database Replication" section on page 7-54. If your output differs from the example in that section, or if you suspect problems or errors in the database installation, try the following:

Step 1 Ensure that the database is installed in the /opt/TimesTen32 directory.

Step 2 Check the log file for installation errors. (The log file is in the directory /opt/TimesTen32/datastore.)

If you find installation errors in the log file, remove and reinstall the CSCOga002 package, as follows:

Step 1 Remove the CSCOga002 package using the **pkgrm** command. To remove the package file, type the following command and press **Enter**:

```
# pkgrm CSCOga002
```

Step 2 Reinstall the package using the **pkgadd** command by typing the following command and pressing **Enter**:

```
# pkgadd -d CSCOga002.pkg
```

If you have questions or need assistance, see the "Obtaining Technical Assistance" section on page xviii.

Restarting the SC Software

After configuring the SC software, you must stop and start the SC software.

Tip If you installed ITK or PTI drivers, the system rebooted and the SC software will be running. If you did not install the drivers, your SC software has not yet been started.

To stop the SC software:

Step 1 As the root user, enter the **/etc/init.d/transpath stop** command.

Step 2 Enter **ps -ef | grep procM** to ensure the software is not running. If you receive no response, the software is stopped.

Note For Software Release 7.4(x), enter **/etc/init.d/CiscoMGC stop** to stop the software.

To start the SC software:

Step 1 As the root user, enter the **/etc/init.d/transpath start** command.

Step 2 Enter **ps -ef | grep procM** to ensure the software is running.

Note For Software Release 7.4(x), enter the **/etc/init.d/CiscoMGC start** command.

Terminating Signaling Links

The SS7 signaling links connect the SC host running Cisco SC software to an SS7 switch. These SS7 signaling links are connected to the Cisco SLT, which connects to the SC host over IP.

If you are upgrading a standalone machine, you can remove the links from your machine and connect them to the Cisco SLTs now.

If you have a high-availability or continuous service configuration, perform these steps:

Step 1 Log in as root to the second SC host that is currently processing calls.

Step 2 Enter the **/etc/init.d/CiscoMGC stop** command to shut down the software. Leave the SC software on the newly upgraded host running.

Caution When you remove the signaling links from the host and terminate them into the Cisco SLT, the host will stop processing calls. Your host will be down until you start the software on the newly upgraded host. You should plan to connect the signaling links during a maintenance window or a low traffic period to minimize call attempt losses.

Note You should coordinate with your SS7 link service provider to let them know that your links will go out of service. Your provider should have on-site support staff available to assist you should there be problems reestablishing the links.

The Cisco SLT requires the Cisco 2611 modular access router with T1 or E1 interfaces running a special release of Cisco IOS software. The Cisco SLT has the following restrictions:

- Only the following Interface Cards are supported. No other cards, or Cisco 2600 or Cisco 3600 series network modules, are supported:
  - 1-port T1 multiflex trunk interface (VWIC-1MFT-T1)
  - 1-port E1 multiflex trunk interface (VWIC-1MFT-E1)
  - 2-port T1 multiflex trunk interface (VWIC-2MFT-T1)
  - 2-port E1 multiflex trunk interface (VWIC-2MFT-E1)
  - 2-port T1 multiflex trunk interface with Drop and Insert (VWIC-2MFT-T1-DI)
  - 2-port E1 multiflex trunk interface with Drop and Insert (VWIC-2MFT-E1-DI)
  - 1-port high-speed serial interface (WIC-1T)
  - 2-port high-speed serial interface (WIC-2T)
- Only SS7 serial interfaces and protocols are supported. There is no support for HDLC, PPP, Frame Relay, ATM, X.25, or other non-SS7 serial WAN protocols.
- Only two SS7 signaling links are supported per Cisco SLT.
- Only one SS7 signaling link is supported per T1 or E1 port.

Moving the Signaling Links in a Standalone Configuration

To move the signaling links, follow these steps:

Step 1 Verify that the Cisco SLT has the WIC that matches your signaling links (either E1 or T1).

Step 2 Connect the Cisco SLT to the Ethernet interface. How you connect to the Cisco SLT will depend on how many SS7 signaling links you have.

If you have one SS7 signaling link, unplug the SS7 signaling link from the ITK card on the SC host and plug it into the WIC on the Cisco SLT.

If you have two SS7 signaling links, follow these steps:

a. Connect Cisco SLT-1 to Ethernet segment 1.

b. Connect Cisco SLT-2 to Ethernet segment 2.

c. Unplug SS7 signaling link #1 from the ITK card on the SC host, and plug it into the WIC on Cisco SLT-1.

d. Unplug SS7 signaling link #2 from the ITK card on the SC host, and plug it into the WIC on Cisco SLT-2.

Step 3 After plugging the links into the Cisco SLT, the carrier detect (CD) light on the back of the Cisco SLT should be green.

Step 4 Stop and start the SC software as described in the "Restarting the SC Software" section on page 7-56.

Step 5 Log in to the SC host, start an MML session, and set the signaling links into service by entering the following MML command:

```
set-sc-state:linkname:IS
```

Where *linkname* is the name you provisioned in the "Terminating Signaling Links" section on page 7-56.

If the signaling links cannot go in-service, back out the new SC software installation using the procedures in the "Migrating Inactive SC Host Configurations" section on page 7-63.

Moving the Signaling Links in a Continuous-Service Configuration

To move the signaling links, follow these steps:

Step 1 Verify that the Cisco SLT has the WIC that matches your signaling links (either E1 or T1).

Step 2 Connect the Cisco SLT to the Ethernet interface. How you connect to the Cisco SLT will depend on how many SS7 signaling links you have.

If you have one SS7 signaling link, unplug the SS7 signaling link from the ITK card on the SC host and plug it into the WIC on the Cisco SLT.

If you have two SS7 signaling links, follow these steps:

a. Connect Cisco SLT-1 to Ethernet segment 1.

b. Connect Cisco SLT-2 to Ethernet segment 2.

c. Unplug SS7 signaling link #1 from the ITK card on the SC host, and plug it into the WIC on Cisco SLT-1.

d. Unplug SS7 signaling link #2 from the ITK card on the SC host, and plug it into the WIC on Cisco SLT-2.

Tip If you have more than 1 link in a linkset, only move 1 link at first to test the functionality. If that link comes up, you can move the other links. If the test link does not come up, move it back to the machine that has not been upgraded and restart the SC software on that machine.

Step 3 After plugging the links into the Cisco SLT, the carrier detect (CD) light on the back of the Cisco SLT should be green.

Step 4 Stop and start the SC software as described in the "Restarting the SC Software" section on page 7-56.

Step 5 Log in to the SC host, start an MML session, and set the signaling links into service by entering the following MML command:

```
set-sc-state:linkname:IS
```

Where *linkname* is the name you provisioned in the "Terminating Signaling Links" section on page 7-56.

If the signaling links cannot go in-service, back out the new SC software installation using the procedures in the "Migrating Inactive SC Host Configurations" section on page 7-63.

Verifying SC Software is Running Properly

To verify that the SC software is running properly you should perform the tests described in the following sections:

- Perform a Test Call and Switchover, page 7-59
- Verifying the Platform State of the SC Hosts, page 7-60
- Verifying the Status of all Signaling Channels, page 7-60
- Verifying the Status of all Traffic Channels, page 7-61
- Verifying the Status of all Destinations, page 7-61
- Checking for Active Alarms, page 7-62
- Verifying Proper Migration of Data, page 7-62

Perform a Test Call and Switchover

Perform the following procedure to test the ability of the software installed on the upgraded SC host to handle a switchover operation:

Note This procedure does not have to be performed on systems with a standalone SC host.

Step 1 Place a test call on your system and hold the call

Step 2 Log in to the other SC host, open an MML session, and enter the following command to perform a manual switchover:

```
sw-over::confirm
```

If the call is sustained, the procedure is complete. Otherwise, proceed to Step 3.

Step 3 Back out the installation of the new SC software, as described in the "Backout Procedures" section on page 7-64.

Verifying the Platform State of the SC Hosts

Ensure that the recently upgraded SC hosts is in the active platform state and that the other SC host is in the standby platform state. If your system uses an SC host in a simplex configuration, the single SC host is always active. To do this, complete the following steps:

Step 1 Log into the upgraded SC host, start an MML session, and enter the following command to determine its platform state:

```
rtrv-ne
```

The system should return a message, similar to the following, if it is currently the active SC host:

```
   Media Gateway Controller 2001-10-10 14:15:22
M  RTRV
   "Type:SC"
   "Hardware platform:sun4u sparc SUNW,Ultra-5_10"
   "Vendor:"Cisco Systems, Inc.""
   "Location:Signaling Controller"
   "Version:"7.4(12)""
   "Platform State:ACTIVE"
```

The valid values for the Platform State field are ACTIVE, STANDBY, or OOS.

Step 2 Log into the other SC host, start an MML session, and enter the following command to determine its platform state:

```
rtrv-ne
```

The system should return a message that indicates that it is in the standby platform state.

If the platform state of either SC host is not correct, check for alarms as described in the "Checking for Active Alarms" section on page 7-62, and take the actions necessary to correct the condition that caused the associated alarm(s).

If the platform state of both SC hosts is active, proceed to Step 3.

Step 3 Contact the Cisco Technical Assistance Center (TAC) for assistance. Refer to the "Obtaining Technical Assistance" section on page xviii for more information on contacting the Cisco TAC.

Verifying the Status of all Signaling Channels

To verify the status of all of the signaling channels and linksets, enter the following command at the active SC host:

```
rtrv-sc:all
```

The system returns a response similar to the following, which shows the signaling links to and from the SC hosts and the associated media gateways.

```
   Media Gateway Controller 2000-03-26 19:23:23
M  RTRV
   "iplink1:nassvc1,LID=0:IS" /* IP Link 1 for NAS 1 */
   "iplink2:nassvc2,LID=0:IS" /* IP Link 1 for NAS 2 */
   "iplink3:nassvc3,LID=0:IS" /* IP Link 1 for NAS 3 */
   "iplink4:nassvc1,LID=0:IS" /* IP Link 2 for NAS 1 */
   "iplink5:nassvc2,LID=0:IS" /* IP Link 2 for NAS 2 */
   "iplink6:nassvc3,LID=0:IS" /* IP Link 2 for NAS 3 */
   "c7iplink1:ls01,LID=0:IS"  /* Link 1 in Linkset 1 */
   "c7iplink2:ls01,LID=1:IS"  /* Link 2 in Linkset 1 */
   "c7iplink3:ls02,LID=0:IS"  /* Link 1 in Linkset 2 */
   "c7iplink4:ls02,LID=1:IS"  /* Link 2 in Linkset 2 */
```

If any of the signaling channels are not in-service, check for alarms as described in the “Checking for Active Alarms” section on page 7-62, and take the actions necessary to correct the condition that caused the associated alarm(s).

Verifying the Status of all Traffic Channels

To verify the status of all of the traffic channels, enter the following command at the active SC host:

```
rtrv-tc:all
```

The system returns a response similar to the following:

```
   Media Gateway Controller - MGC-01 2000-04-05 08:26:36
M  RTRV
   "dpc1:CIC=1,PST=IS,CALL=IDLE,BLK=NONE"
   "dpc1:CIC=2,PST=IS,CALL=IDLE,BLK=NONE"
   "dpc1:CIC=3,PST=IS,CALL=IDLE,BLK=NONE"
   "dpc1:CIC=4,PST=IS,CALL=IDLE,BLK=NONE"
   "dpc1:CIC=5,PST=IS,CALL=IDLE,BLK=NONE"
   "dpc1:CIC=6,PST=IS,CALL=IDLE,BLK=NONE"
   "dpc1:CIC=7,PST=IS,CALL=IDLE,BLK=NONE"
   "dpc1:CIC=8,PST=IS,CALL=IDLE,BLK=NONE"
   "dpc1:CIC=9,PST=IS,CALL=IDLE,BLK=NONE"
```

If any of the traffic channels are not in-service, check for alarms as described in the “Checking for Active Alarms” section on page 7-62, and take the actions necessary to correct the condition that caused the associated alarm(s).

Verifying the Status of all Destinations

To verify the status of all of the destination point codes (DPCs) provisioned on your SC host, enter the following command at the active SC host:

```
rtrv-dest:all
```

The system returns a response similar to the following:

```
   Media Gateway Controller - MGC-04 2000-04-05 08:05:36
M  RTRV
   "dpc1:PKG=SS7-ANSI,ASSOC=SWITCHED,PST=IS,SST=UND"
   "dpc2:PKG=SS7-ANSI,ASSOC=SWITCHED,PST=IS,SST=UND"
   "dpc3:PKG=SS7-ANSI,ASSOC=SWITCHED,PST=IS,SST=UND"
   "dpc4:PKG=SS7-ANSI,ASSOC=SWITCHED,PST=IS,SST=UND"
   "dpc5:PKG=SS7-ANSI,ASSOC=SWITCHED,PST=IS,SST=UND"
   "dpc6:PKG=SS7-ANSI,ASSOC=SWITCHED,PST=IS,SST=UND"
```

Note If the **rtrv-dest:all** MML command is entered soon after a switchover has occurred, the state of some of the destinations might be listed as undefined (UND). UND is the default state for a destination when the system starts. In this instance, UND states indicate that the SC host has not received a service state message from the associated destination since the switchover occurred. No user action is required.

If any of the DPCs are not in-service, check for alarms as described in the “Checking for Active Alarms” section on page 7-62, and take the actions necessary to correct the condition that caused the associated alarm(s).

Checking for Active Alarms

To retrieve all active alarms, enter the following command at the active SC host:

```
rtrv-alms
```

The system returns a response that shows all active alarms, in a format similar to the following:

```
Media Gateway Controller 2000-02-26 11:41:01
M  RTRV
   "LPC-01: 2000-02-26 09:16:07.806,"
   "LPC-01:ALM=\"SCMGC MTP3 COMM FAIL\",SEV=MJ"
   "IOCM-01: 2000-02-26 09:17:00.690,"
   "IOCM-01:ALM=\"Config Fail\",SEV=MN"
   "MGC1alink2: 2000-02-26 09:17:47.224,ALM=\"SC FAIL\",SEV=MJ"
   "MGC1alink3: 2000-02-26 09:17:47.225,ALM=\"SC FAIL\",SEV=MJ"
   "MGC1alink4: 2000-02-26 09:17:47.226,ALM=\"SC FAIL\",SEV=MJ"
   "MGC2alink1: 2000-02-26 09:17:47.227,ALM=\"SC FAIL\",SEV=MJ"
   "MGC2alink2: 2000-02-26 09:17:47.227,ALM=\"SC FAIL\",SEV=MJ"
   "MGC2alink4: 2000-02-26 09:17:47.229,ALM=\"SC FAIL\",SEV=MJ"
   "dpc5: 2000-02-26 09:17:47.271,ALM=\"PC UNAVAIL\",SEV=MJ"
   "ls3link1: 2000-02-26 09:16:28.174,"
   "ls3link1:ALM=\"Config Fail\",SEV=MN"
   "ls3link1: 2000-02-26 09:18:59.844,ALM=\"SC FAIL\",SEV=MJ"
```

If any alarms are present, determine whether you need to take corrective action to resolve the alarm condition. The alarms that require corrective action are listed in the *Alarm Troubleshooting Procedures* section of the *Cisco MGC Node Troubleshooting* chapter in the *Cisco Media Gateway Controller Software Release 7 Operations, Maintenance, and Troubleshooting Guide*. Information on all alarms can be found in the *Cisco Media Gateway Controller Software Release 7 Messages Reference Guide*.

Verifying Proper Migration of Data

Verify that the contents of the XECfgParm.dat file and the active configuration file have successfully migrated by performing the following steps:

Step 1 Verify the contents of the XECfpParm.dat file in the upgraded SC host, using the procedure in the Opening the XECfgParm.dat File, page 7-20, ensuring that the parameter settings from your previous release of the SC software have migrated properly (migrated properties are indicated by the comment “migrated” after the parameter).

If the parameter settings have not migrated properly, correct the value of the parameters and save the file, as described in the “Saving the XECfgParm.dat File” section on page 7-37. Otherwise, proceed to Step 2.

Note For more information on the settings for the XECfgParm.dat parameters, refer to the *Cisco Media Gateway Controller Software Release 7 Installation and Configuration Guide*.

Step 2 Enter the following UNIX commands to launch the Cisco MGC toolbar:

```
cd /opt/CMM/bin
```

```
./start.sh tool
```

The MGC Toolbar window is displayed.

Step 3 Click **CONFIG-LIB** on the Cisco MGC toolbar to open the Config-Lib viewer window.

Step 4 Enter 1 at the prompt to list the configuration versions in the library.

If the configuration identified in the Config-Lib viewer window as the current production version matches the name of your active configuration, the procedure is complete.

If the configuration identified in the Config-Lib viewer window as the current production version does *not* match the name of your active configuration, proceed to Step 5.

Step 5 Check the list of configurations in the Config-Lib viewer window to determine whether the name of your active configuration is listed.

If your active configuration is not listed in the Config-Lib viewer window, proceed to Step 6.

If your active configuration is listed in the Config-Lib viewer window, proceed to Step 8.

Step 6 Manually migrate the old SC host configurations using the procedure described in the "Migrating Inactive SC Host Configurations" section on page 7-63.

Step 7 Exit and re-open the Config-Lib viewer window to load the retrieved configurations into the viewer window.

Step 8 Stop the SC software using the following UNIX command:

```
etc/init.d/CiscoMGC stop
```

Step 9 Once the SC software has stopped completely, return to the Config-Lib viewer window and enter 3 at the prompt and enter the number of the library version to be set as the active configuration.

Step 10 Restart the SC software using the following UNIX command:

```
etc/init.d/CiscoMGC start
```

Step 11 Exit and re-open the Config-Lib viewer window. Ensure that the active configuration is now correct. If the active configuration is still not correct, proceed to Step 12. Otherwise, the procedure is complete.

Step 12 Contact the Cisco TAC for assistance. Refer to the "Obtaining Technical Assistance" section on page xviii for more information on contacting the Cisco TAC.

Migrating Inactive SC Host Configurations

When installing the SC software, only the active configuration files (located in /opt/CiscoMGC/etc) are migrated. You can use the migrate script to migrate old configurations to a new version. To use the migrate script:

Step 1 Log in to the SC host.

Step 2 Enter the following command:

```
migrate top-leveldirectory sourcedirectory destinationdirectory
```

Top-leveldirectory is the software directory. For Software Release 7.3(x), it is /opt/TransPath; for Software Release 7.4(x), it is /opt/CiscoMGC. *Sourcedirectory* is the relative path of the directory that you want to migrate. *Destinationdirectory* is the relative path of the directory into which the migrated files are copied. If the directory does not exist, the migrate script creates it. If the directory exists, you are prompted to overwrite it.

Backout Procedures

If the SC software upgrade did not work properly, perform the following steps:

Step 1 If you are upgrading a Cisco SS7 DAS Release 2.0 system in a high-availability configuration, remove the signaling links from the Cisco SLTs. Terminate them back into the ITK cards in your standby SC host (that has not been upgraded).

Step 2 Log in as root to the standby SC host and restart the software by entering **/etc/init.d/transpath start**.

Note Enter **/etc/init.d/CiscoMGC start** on an SC host running Release 7.4(x).

Step 3 In a simplex configuration, perform the following steps:

a. Uninstall the new SC software.

b. If you are upgrading a Cisco SS7 DAS Release 2.0 system, uninstall the Solaris 2.6 software and then reinstall Solaris 2.5.

c. Reinstall the previous version of SC software.

d. Restore your backed up files, as described in the “Restoring Your SC Host Data” section on page 7-64.

e. If you are upgrading a Cisco SS7 DAS Release 2.0 system, remove the signaling links from the Cisco SLTs and terminate them into the SC host.

Restoring Your SC Host Data

Use the procedures in these sections to restore the SC data you previously backed up. If you backed up your data to tape, see the “Restoring Your Data from a Local Tape Drive” section on page 7-64. If you backed up your data to a remote machine using the IP network, see the “Restoring Your Data from a Remote Machine” section on page 7-65.

Restoring Your Data from a Local Tape Drive

This procedure restores everything on a tape installed in the local tape drive to the SC software base directory. This procedure assumes the operating system has just been installed and no SC software has been loaded. This procedure returns the etc and dialPlan subdirectories from a tape in the local tape drive to the /opt/TransPath directory. When the new SC software is later installed, it detects these files and uses them to migrate to the new configuration.

Step 1 Log in to the system as root and enter the following UNIX command at the affected Cisco MGC to run the restore script:

```
# ./restore.sh
```

The system returns a response similar to the following:

```
MGC restore utility
-----------------------------
Source currently set to Local tape (/dev/rmt/0h)
Enter:
    <N> set source to remote NFS server
    <L> set source to Local tape (/dev/rmt/0h)
    <R> for Restore
    <Q> to quit
Select restore mode:
```

Step 2 Select **R** and press **Enter** to start the restore. The system then prompts you as listed below:

```
Are you sure you want to restore a backup.
Current data in the MGC directory will be overwritten and lost.

Answer(Y/N):
```

Step 3 Select **y** and press **Enter** if you are sure you want to restore from the tape. The system begins the restoration and returns a response similar to the following:

```
Answer(Y/N): y
x ., 0 bytes, 0 tape blocks
x ./var, 0 bytes, 0 tape blocks
x ./var/log, 0 bytes, 0 tape blocks
x ./var/log/platform.log, 117 bytes, 1 tape blocks
x ./var/log/mml.log, 187 bytes, 1 tape blocks.
.
.
.
#
```

Step 4 When the restore has finished, remove the tape from the tape drive.

Step 5 If your system does not have a dial plan configured, the procedure is complete. Otherwise, restore the contents of your dial plan as described in the "Restoring Data to the Main Memory Database" section on page 7-67.

This completes restoring your SC host data from a local tape drive.

Restoring Your Data from a Remote Machine

This procedure restore files from the etc and dialPlan subdirectories to the /opt/CiscoMGC directory from a file on an NFS mountable directory on remote machine. The remote machine must be set up with an NFS mountable directory that is writable by machine being backed up. The NFS set up of the remote machine is beyond the scope of this procedure. When the new SC software is later installed, it detects these files and uses them to migrate to the new configuration.

Step 1 Log in to the system as root and enter the following UNIX command on the affected Cisco MGC to run the restore script:

```
# ./restore.sh
```

The system returns a response similar to the following:

```
MGC restore utility
-----------------------------
Source currently set to Local tape (/dev/rmt/0h)
Enter:
    <N> set source to remote NFS server
    <L> set source to Local tape (/dev/rmt/0h)
    <R> for Restore
    <Q> to quit
Select restore mode:
```

Step 2 Select **N** and press **Enter** to define the remote NFS server. The system then prompts you to provide the name of the remote server.

Step 3 Enter the name of the remote NFS server:

```
Enter server name: remote_hostname
```

Where: *remote_hostname*—Name of the remote server where the backups are stored.

The system then prompts you to enter the name of the associated directory on the remote server.

Step 4 Enter the directory name on the remote NFS server:

```
Enter remote directory : remote_directory_name
```

Where: *remote_directory_name*—Name of the directory path on the remote server where the backups are stored.

The system returns a response similar to the following:

```
Enter server name: va-panthers
Enter remote directory : /backup

MGC restore utility
-----------------------------

Source currently set to remote NFS server (va-panthers:/backup)
Enter:

    <N> set source to remote NFS server
    <L> set source to Local tape (/dev/rmt/0h)
    <R> for Restore
    <Q> to quit
```

The system then prompts you to select the restore mode.

```
Select restore mode:
```

Step 5 Select **R** and press **Enter** to start the restore. The system returns a response similar to the following:

```
mount -F nfs -o retry=3 va-panthers:/backup /mnt

Available files:
va-blade20000317105201P.tar
va-blade20000317105337.tar
```

The system then prompts you to enter the filename to be restored.

```
Enter filename to restore from:
```

Step 6 Enter the filename for the most recent full backup performed on your system.

Note Full backups have a file name consisting of the name of the host and the timestamp with a .tar designation. Partial backups have a file name consisting of the name of the host, timestamp, and the letter "P" with a .tar designation.

The system then asks you if you really want to restore a backup:

```
Are you sure you want to restore a backup.
Current data in the MGC directory will be overwritten and lost.

Answer(Y/N):
```

Step 7 Enter **y** and press **Enter** if you are sure that you want to restore the Cisco MGC directory. The system returns a response similar to the following:

```
x etc, 0 bytes, 0 tape blocks
x etc/Copyright, 545 bytes, 2 tape blocks
x etc/CONFIG_LIB, 0 bytes, 0 tape blocks
x etc/CONFIG_LIB/new, 0 bytes, 0 tape blocks
.
.
restore from va-panthers:/backup/va-blade20000317105337.tar complete
#
```

Step 8 If your system does not have a dial plan configured, the procedure is complete. Otherwise, restore the contents of your dial plan as described in the "Restoring Data to the Main Memory Database" section on page 7-67.

Restoring Data to the Main Memory Database

Use this procedure to restore your dial plan data.

Step 1 Change directories to a local subdirectory under the base directory.

For example, enter the following UNIX command to change to the /opt/CiscoMGC/local directory:

```
cd /opt/CiscoMGC/local
```

Step 2 Run the MMDB restore script by entering the following UNIX command:

```
./restoreDb.sh filename
```

Where *filename* is the name of the database backup file.

For example, to restore the contents of a file called dplan to the MMDB, you would enter the following command:

```
./restoreDb.sh dplan
```

The system returns a response similar to the following:

```
Restoring database contents for DSN=howdydb into dplan
The Restore process is being initiated for the datastore howdydb
Files for /opt/TimesTen32/datastore/howdydb are being restored up onto standard output
Restore Complete
```

Resetting the Configuration

Once the upgrade is complete on the second SC host, you must return to the first SC host you upgraded and reset its configuration to enable it to synchronize with the second SC host. To do this, perform the following steps:

Step 1 Open the XECfgParm.dat file on the first SC host, as described in the "Opening the XECfgParm.dat File" section on page 7-20, and change the value of pom.dataSync to **true**.

Step 2 Save your changes and exit the file.

Step 3 Stop the SC software using the following UNIX command:

```
etc/init.d/CiscoMGC stop
```

Step 4 Once the SC software has stopped completely, restart the SC software using the following UNIX command:

```
etc/init.d/CiscoMGC start
```

Provisioning the Configuration

Note If you are upgrading from the Cisco SS7 DAS Release 2.0, you should provision your configuration again. Although provisioning data is migrated from Software Release 4 to Software Release 7.x, it is likely that your old configuration will not work with the new software. You must provision your configuration again and commit or deploy it to the active SC host.

After installing the new software on the SC host, you may need to add provisioning information to your configuration using MML or your GUI provisioning tool. If you added Cisco SLTs, you must provision these into the configuration. You should have the names of the components in your solution available. For more information, see the "Gathering Provisioning Data" section on page 1-4.

For an overview of provisioning and instructions to assist you, see *Cisco Media Gateway Controller Software Release 7 Provisioning Guide*. For instructions on provisioning a sample Cisco SS7 Interconnect for Access Servers Solution, see the appropriate provisioning guide for your solution.

Timesaver To save time, you can use an MML batch file to provision your system. This requires that you enter all MML commands to provision your system into an ASCII text file and import the file. See the see the appropriate provisioning guide for your solution for more information and a sample batch file.

Tip The SC software must be running in order to provision the system. If you encounter problems, make sure the software is running. Refer to the "Restarting the SC Software" section on page 7-56.

INDEX