



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

December 29, 2003

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

Text Part Number: OL-0542-06



THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

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

All other trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0304R)

Cisco Media Gateway Controller Software Release 7 Operations, Maintenance, and Troubleshooting Guide
Copyright © 2000-2003 Cisco Systems, Inc.
All rights reserved.

Preface ix

Document Objective	ix
Audience	x
Document Organization	x
Conventions	xi
Documentation Suite	xiv
Related Documentation	xv
Obtaining Documentation	xvii
Cisco.com	xvii
Ordering Documentation	xvii
Documentation Feedback	xvii
Obtaining Technical Assistance	xviii
Cisco TAC Website	xviii
Opening a TAC Case	xviii
TAC Case Priority Definitions	xviii
Obtaining Additional Publications and Information	xix
Document Change History	xix

CHAPTER 1**Cisco MGC System Overview 1-1**

Cisco Media Gateway Controller Node	1-1
Cisco Media Gateway Controller	1-1
Cisco Signaling Link Terminals	1-2
Cisco Catalyst 5500 Multiswitch Routers	1-2
Cisco MGC Software Architecture	1-3
Input/Output Subsystem	1-5
Element Management Subsystem	1-5
Fault Tolerance Subsystem	1-6
Execution Environment Process Shell	1-7
Call Engine Process	1-8
Call Instance Component	1-8
Cisco MGC Software Directory Structure	1-10

CHAPTER 2**Cisco MGC Node Component Startup and Shutdown Procedures 2-1**

Cisco Media Gateway Controller Startup Procedures	2-1
Starting the Cisco MGC Hardware	2-2
Starting the Cisco MGC Software	2-2
Cisco Signaling Link Terminal Startup Procedure	2-3
Cisco Catalyst 5500 Multiswitch Router Startup Procedure	2-3

Cisco Media Gateway Controller Shutdown Procedure	2-4
Shutting Down the Cisco MGC Software Manually	2-4
Shutting Down the Cisco MGC Hardware	2-4
Cisco Signaling Link Terminal Shutdown Procedure	2-5
Cisco Catalyst 5500 Multiswitch Router Shutdown Procedure	2-5

CHAPTER 3

Cisco MGC Node Operations 3-1

Daily Tasks	3-1
Starting an MML Session	3-2
Verifying the Platform State of the Cisco MGC Hosts	3-2
Verifying That Processes Are Running	3-3
Monitoring the Alarms Status	3-6
Verifying the Status of all Destinations	3-8
Verifying State of all SS7 Routes	3-10
Verifying CIC States	3-13
Verifying Available Disk Space	3-17
Verifying Available Virtual Memory	3-17
Verifying Available RAM	3-19
Verifying CPU Utilization Level	3-19
Verifying the Number of Active Processes	3-21
Verifying the Number of Users	3-22
Verifying Available Memory on the Cisco SLTs	3-23
Periodic Maintenance Procedures	3-23
Automatic Disk Space Monitoring	3-24
Automatic System Log Rotation	3-27
Rotating System Logs Manually	3-27
Creating a Disaster Recovery Plan	3-27
Backing Up System Software	3-28
Regular Operations	3-39
Managing MML Sessions	3-39
Managing Signaling Channels	3-47
Managing Bearer Channels	3-55
Provisioning your Cisco MGC	3-63
Managing your Cisco MGC Platform	3-80
Managing System Measurements	3-90
Using the Cisco MGC Viewer Toolkit	3-102

CHAPTER 4

Maintenance and Troubleshooting Overview 4-1

Maintenance Strategy Overview	4-1
-------------------------------	-----

Troubleshooting Strategy Overview	4-2
Symptoms, Problems, and Solutions	4-2
General Problem-Solving Model	4-2
System Troubleshooting Tools	4-4
Third-Party Troubleshooting Tools	4-9

CHAPTER 5**Maintaining the Cisco MGC 5-1**

Checking Equipment Status	5-1
Sun Netra LEDs	5-1
Sun Enterprise 450 LEDs	5-2
Maintaining Technical Support Staff	5-3
Skill Level of Personnel	5-3
Staff Software Troubleshooting Tools	5-3
Maintaining Components	5-3
Software Upgrades	5-3

CHAPTER 6**Maintaining the Cisco Signaling Link Terminal 6-1**

Checking Equipment Status	6-2
Cisco SLT LEDs	6-2
Using the Cisco SLT Operating System to Check Status	6-4
Removing a Cisco SLT	6-5
Required Tools and Equipment	6-5
Procedure	6-6
Replacing a Cisco SLT	6-6
Required Tools and Equipment	6-6
Mounting the Chassis in a Rack	6-6
Connecting the DC Power Supply	6-9
Connecting to a Network	6-11
Connecting the Console Terminal and Modem	6-11
Cisco SLT Interface Numbering	6-12
Install the New Software	6-13
Replacing Hardware Components	6-13
Required Tools and Equipment	6-14
Installing a WAN Interface Card	6-14
Additional Maintenance Tasks	6-15
Upgrading DRAM	6-16
Replacing the System-Code SIMM	6-19
Closing the Chassis	6-21
Procedures for Recovering Boot and System Images	6-22

CHAPTER 7

Maintaining the Cisco Catalyst 5500 Multiswitch Router 7-1

- Checking Equipment Status 7-1
 - Cisco Catalyst 5500 LEDs 7-1
 - Using the Command Line Interface to Check Status 7-5
- Replacing Hardware Components 7-5
 - Avoiding Problems When Inserting and Removing Modules 7-6
 - Tools Required 7-6
 - Removing the Supervisor Engine 7-6
 - Replacing the Supervisor Engine 7-7
 - Using Flash Memory (PCMCIA) Cards (Supervisor Engine III) 7-7
 - Removing and Replacing the Power Supply 7-8
 - Installing an AC-Input Power Supply 7-10
 - Removing a DC-Input Power Supply 7-11
 - Installing a DC-Input Power Supply 7-13
 - Removing and Replacing the Chassis Fan Assembly 7-15

CHAPTER 8

Troubleshooting the Cisco MGC Node 8-1

- Troubleshooting Overview 8-1
 - Cisco SLT Failure 8-2
 - Cisco MGC Failure 8-2
 - Operating System Failure 8-2
- Troubleshooting Using Cisco MGC Alarms 8-2
 - Retrieving All Active Alarms 8-3
 - Acknowledging Alarms 8-3
 - Clearing Alarms 8-4
 - Troubleshooting with System Logs 8-4
 - Alarm Troubleshooting Procedures 8-8
- SS7 Network Related Problems 8-50
 - Signaling Channel Problems 8-51
 - Signaling Destination Problems 8-55
 - SS7 Network Troubleshooting Procedures 8-58
- Bearer Channel Connection Problems 8-69
 - Troubleshooting Bearer Channel Connection Procedures 8-70
- Tracing 8-102
 - Performing a Call Trace 8-102
 - Alternatives to Call Tracing 8-108
 - Performing a TCAP Trace 8-111
- Platform Troubleshooting 8-112

Deleting Unnecessary Files to Increase Available Disk Space	8-112
Recovering from a Switchover Failure	8-113
Recovering from Cisco MGC Host(s) Failure	8-115
Restoring Stored Configuration Data	8-117
Verifying Proper Configuration of Replication	8-123
Measurements Are Not Being Generated	8-123
Call Detail Records Are Not Being Generated	8-123
Rebooting Your System to Modify Properties	8-124
Rebooting Software to Modify Configuration Parameters	8-125
Resolving a Failed Connection to a Peer	8-125

APPENDIX A**Configuring Cisco MGC Report Files A-1**

Understanding Logging Files	A-1
Configuring the Data Dumper	A-2
Configuring the Data Dumper to Support BAMS	A-5
Understanding the Format of Log Files Archived Using Data Dumper	A-6

APPENDIX B**Troubleshooting Cisco SLT Signaling B-1**

Cisco SLT Signaling Overview	B-2
IP Signaling Backhaul	B-2
Connection Management	B-3
Troubleshooting SS7 Link Problems	B-4
Checking Link Configuration Files	B-5
Checking UDP Traffic Flows	B-5
Checking Connection between Cisco MGC and Cisco SLT	B-6
Checking the T1/E1 Link State	B-6
Verifying the Link Alignment Status	B-6
Verifying Exchanged Point Codes	B-7
Cross-Checking Configuration Files	B-8
Troubleshooting Cisco SLT-to-STP Signaling Links	B-10
MTP1 Communication Problems	B-11
MTP2 Communication Problems	B-12
Troubleshooting Cisco SLT to Cisco MGC Communications	B-13
Identifying MTP3 and Higher Layer Problems	B-13
Identifying Ethernet Connectivity Problems	B-14
Identifying IP Communication Problems	B-14
Cisco SLT Error Messages	B-15

APPENDIX C

Troubleshooting Cisco Catalyst 5500 Multiswitch Routers Signaling C-1

MSR VLANs **C-1**

Command Line Interface **C-2**

Command Line Interface Local Access **C-3**

Command Line Interface Remote Access **C-3**

Troubleshooting MSR Virtual Pathways and ISLs **C-3**

APPENDIX D

Cisco Media Gateway Controller Measurements D-1

ANSI ISUP Measurements **D-12**

INDEX



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 Objective, page ix
- Audience, page x
- Document Organization, page x
- Conventions, page xi
- Documentation Suite, page xiv
- Obtaining Documentation, page xvii
- Documentation Feedback, page xvii
- Obtaining Technical Assistance, page xviii
- Obtaining Additional Publications and Information, page xix
- Document Change History, page xix

Document Objective

This document provides instructions for operating, maintaining, and troubleshooting the core elements of the Cisco Media Gateway Controller (MGC) node, as listed below.

- Cisco MGCs
- Cisco Signaling Link Terminals (SLTs)
- Cisco Catalyst Multiswitch Routers (MSRs)

This document covers such topics systems operation and management, signaling channel operation, alarm management, and problem identification and resolution. The procedures in this document are to be used when your Cisco MGC node is configured with two Cisco MGCs working in a continuous service mode, unless otherwise specified.



Note

The term *media gateway controller* used in this document is a generic term that applies to both the Cisco SC2200 Signaling Controller and the Cisco PGW 2200 products. Some of the documentation for your telephony solution might use the terms signaling controller and PSTN Gateway to refer to features that are unique to the separate products.

**Note**

The Cisco PGW 2200 was formerly known as the Cisco VSC3000 Virtual Switch Controller. Some parts of this document may use this older name.

Audience

This guide is intended for three audiences: the system administrators, the system operators, and the system technicians.

- The system administrator manages the host administrative functions, including configuring and maintaining system parameters, granting group and user IDs, and managing all Cisco MGC files and directories. The system administrator should have an in-depth knowledge of UNIX and a basic knowledge of data and telecommunications networking.
- The system operator should be familiar with telecommunication protocols, basic computer software operations, computer terminology and concepts, hierarchical file systems, common UNIX shell commands, log files, and the configuration of telephony switching systems.
- The system technician should be familiar with telecommunication protocols, basic computer software operations, computer terminology and concepts, hierarchical file systems, common UNIX shell commands, log files, the configuration of telephony switching systems, the use of electrical and electronic telephony test equipment, and basic troubleshooting techniques.

Document Organization

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

Table 1 *Major Sections of This Guide*

Chapter/ Appendix	Title	Description
Chapter 1	Cisco MGC System Overview	Includes high-level descriptions of the operations, maintenance, and troubleshooting procedures contained in this guide.
Chapter 2	Cisco MGC Node Component Startup and Shutdown Procedures	Contains the recommended startup and shutdown procedures for each component of the Cisco MGC node.
Chapter 3	Cisco MGC Node Operations	Explains how to manage Cisco MGC operations, including starting and stopping the application, running the process manager, operating the switchover process, retrieving signal channel attributes, and changing signal service states.
Chapter 4	Maintenance and Troubleshooting Overview	Contains the overall maintenance strategies for the Cisco MGC node.
Chapter 5	Maintaining the Cisco MGC	Describes maintenance of the Cisco MGC hosts, including LED descriptions, shutdown and restart procedures, spare parts stocking levels, the log rotation utility, the diskmonitor program, and backup procedures.

Table 1 *Major Sections of This Guide (continued)*

Chapter/ Appendix	Title	Description
Chapter 6	Maintaining the Cisco Signaling Link Terminal	Describes maintenance of the Cisco SLT, including checking equipment status, replacing a complete signal processor, replacing hardware components, and performing other maintenance tasks.
Chapter 7	Maintaining the Cisco Catalyst 5500 Multiswitch Router	Describes maintenance of Cisco Catalyst MSRs, including checking equipment status, replacing a complete router, and replacing various components.
Chapter 8	Troubleshooting the Cisco MGC Node	Describes strategies for isolating problems, including the use of system alarms, indicators, and interfaces. Explains how to troubleshoot the Cisco MGC. Troubleshooting includes working with alarms and resolving signaling channel problems, signaling destination problems, and bearer connection problems. System logs are also described.
Appendix A	Configuring Cisco MGC Report Files	Describes the Cisco MGC log files: how to view, print, and interpret log files. Also explains how to use the Cisco MGC software to retrieve network measurements and statistics, including call detail, measurement, and alarm records.
Appendix B	Troubleshooting Cisco SLT Signaling	Explains how to troubleshoot the Cisco SLTs, including Cisco SLT to STP signaling links and Cisco SLT to Cisco MGC signaling links.
Appendix C	Troubleshooting Cisco Catalyst 5500 Multiswitch Routers Signaling	Describes troubleshooting the Cisco MSR using the command line interface, as well as virtual pathways and links.
Appendix D	Cisco Media Gateway Controller Measurements	Lists the measurements used by the Cisco MGC.

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
<i>Italics</i>	Variables for which you supply values	command <i>type interface</i> 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 ()	Separated alternative elements	command [abc def] You can choose either abc or def, or neither, but not both.
Braces ({ })	Required choices	command { abc def } You must use either abc or def, but not both.
Braces and vertical bars within square brackets ([{ }])	A required choice within an optional element	command [abc { def 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 you are setting an SNMP community string to <i>public</i> , 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	
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 guide.

**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 –21000000001
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."

Table 3 *Data Type Conventions (continued)*

Data Type	Definition	Example
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
Note	All known exceptions to these conventions are expressed in the specific format sections of this document.	

Documentation Suite

The documents that make up the Cisco MGC documentation set are listed in Table 4. The grayed box in this table indicates the publication you are currently reading.

Table 4 *Cisco MGC Documentation*

Functional Area	Publication	Description and Audience
Hardware Installation	<i>Cisco Media Gateway Controller Hardware Installation Guide</i>	Describes how to install the hardware components of the Cisco MGC node. Includes detailed information on the environmental requirements for all the components and step-by-step hardware installation and operational verification procedures. Also provides a checklist of the hardware you should have before starting the installation and a checklist of all the connections for the components. The audience for these publications is the engineering personnel responsible for installing the components and verifying the hardware installation.
Software Installation	<i>Cisco Media Gateway Controller Software Release 7 Installation and Configuration Guide</i>	Describe the steps necessary to install and upgrade the software components of the Cisco MGC. The audience for these publications is the engineering personnel responsible for installing, configuring, and upgrading software for the respective solutions.
Software Release Notes	<i>Release Notes for the Cisco Media Gateway Controller Software Release 7</i>	Provides information that is specific to a particular release of the Cisco MGC software. The audience for these publications is the engineering personnel responsible for installing, configuring, and upgrading software for the respective solutions.

Table 4 *Cisco MGC Documentation (continued)*

Functional Area	Publication	Description and Audience
Provisioning	<i>Cisco Media Gateway Controller Software Release 7 Provisioning Guide</i>	Provide step-by-step procedures for provisioning the Cisco MGC.
	<i>Cisco Media Gateway Controller Software Release 7 Dial Plan Guide</i>	The audience for these publications is the engineering personnel responsible for provisioning.
Operations, Maintenance, and Troubleshooting	<i>Cisco Media Gateway Controller Software Release 7 Operations, Maintenance, and Troubleshooting Guide</i>	Describes the procedures necessary to conduct day-to-day operations, to perform preventive and corrective maintenance, and to troubleshoot the various components of the solution. The audience for this publication is the system administrators, system operators, and service technicians responsible for operating, maintaining, and servicing the components of the respective solutions
Reference	<i>Regulatory Compliance and Safety Information for the Cisco Media Gateway Controller Hardware</i>	Provide reference information for the hardware and software of the Cisco MGC.
	<i>Cisco Media Gateway Controller Software Release 7 MML Command Reference Guide</i>	The audience for these publications is the engineering personnel responsible for installing, configuring, operating and upgrading software for the respective solutions.
	<i>Cisco Media Gateway Controller Software Release 7 Messages Reference Guide</i>	
	<i>Cisco Media Gateway Controller Software Release 7 Billing Interface Guide</i>	
	<i>Cisco Media Gateway Controller Software Release 7 Management Information Base Guide</i>	

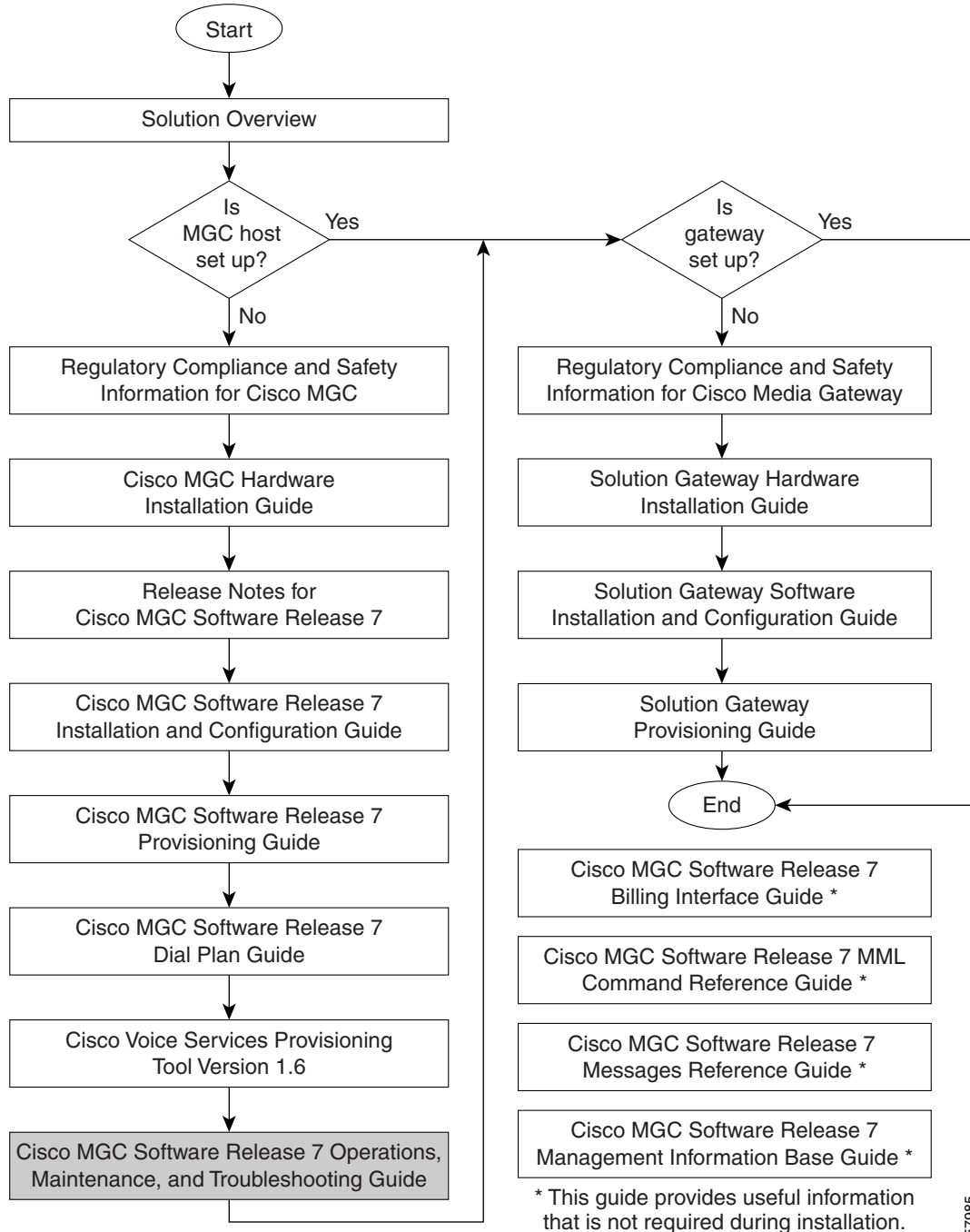
Related Documentation

Other useful reference publications include

- Overviews of the related telephony solutions—Describe the Cisco telephony solutions with which the Cisco MGC node is associated
- Provisioning guides for the related telephony solutions—Describe the provisioning steps for the Cisco telephony solutions with which the Cisco MGC node is associated
- Solution gateway installation and configuration guides—Describe how to install and configure the media gateway for a particular Cisco telephony solution.

Figure 1 shows the sequence in which the various manuals documenting Cisco telephony solutions should be read.

Figure 1 Documentation Roadmap



57985

Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. Cisco also provides several ways to obtain technical assistance and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

Cisco.com

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

<http://www.cisco.com/univercd/home/home.htm>

You can access the Cisco website at this URL:

<http://www.cisco.com>

International Cisco websites can be accessed from this URL:

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

Ordering Documentation

You can find instructions for ordering documentation at this URL:

http://www.cisco.com/univercd/cc/td/doc/es_inpk/pdi.htm

You can order Cisco documentation in these ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Ordering tool:
<http://www.cisco.com/en/US/partner/ordering/index.shtml>
- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, USA) at 408 526-7208 or, elsewhere in North America, by calling 800 553-NETS (6387).

Documentation Feedback

You can submit e-mail comments about technical documentation to bug-doc@cisco.com.

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

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

We appreciate your comments.

Obtaining Technical Assistance

For all customers, partners, resellers, and distributors who hold valid Cisco service contracts, the Cisco Technical Assistance Center (TAC) provides 24-hour-a-day, award-winning technical support services, online and over the phone. Cisco.com features the Cisco TAC website as an online starting point for technical assistance. If you do not hold a valid Cisco service contract, please contact your reseller.

Cisco TAC Website

The Cisco TAC website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The Cisco TAC website is available 24 hours a day, 365 days a year. The Cisco TAC website is located at this URL:

<http://www.cisco.com/tac>

Accessing all the tools on the Cisco TAC website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a login ID or password, register at this URL:

<http://tools.cisco.com/RPF/register/register.do>

Opening a TAC Case

Using the online TAC Case Open Tool is the fastest way to open P3 and P4 cases. (P3 and P4 cases are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Case Open Tool automatically recommends resources for an immediate solution. If your issue is not resolved using the recommended resources, your case will be assigned to a Cisco TAC engineer. The online TAC Case Open Tool is located at this URL:

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

For P1 or P2 cases (P1 and P2 cases are those in which your production network is down or severely degraded) or if you do not have Internet access, contact Cisco TAC by telephone. Cisco TAC engineers are assigned immediately to P1 and P2 cases to help keep your business operations running smoothly.

To open a case by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)

EMEA: +32 2 704 55 55

USA: 1 800 553-2447

For a complete listing of Cisco TAC contacts, go to this URL:

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

TAC Case Priority Definitions

To ensure that all cases are reported in a standard format, Cisco has established case priority definitions.

Priority 1 (P1)—Your network is “down” or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Priority 2 (P2)—Operation of an existing network is severely degraded, or significant aspects of your business operation are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Priority 3 (P3)—Operational performance of your network is impaired, but most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Priority 4 (P4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- Cisco Marketplace provides a variety of Cisco books, reference guides, and logo merchandise. Go to this URL to visit the company store:
<http://www.cisco.com/go/marketplace/>
- The Cisco *Product Catalog* describes the networking products offered by Cisco Systems, as well as ordering and customer support services. Access the Cisco Product Catalog at this URL:
<http://cisco.com/univercd/cc/td/doc/pcat/>
- *Cisco Press* publishes a wide range of general networking, training and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press online at this URL:
<http://www.ciscopress.com>
- *Packet* magazine is the Cisco quarterly publication that provides the latest networking trends, technology breakthroughs, and Cisco products and solutions to help industry professionals get the most from their networking investment. Included are networking deployment and troubleshooting tips, configuration examples, customer case studies, tutorials and training, certification information, and links to numerous in-depth online resources. You can access Packet magazine at this URL:
<http://www.cisco.com/packet>
- *iQ Magazine* is the Cisco bimonthly publication that delivers the latest information about Internet business strategies for executives. You can access iQ Magazine at this URL:
<http://www.cisco.com/go/iqmagazine>
- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:
<http://www.cisco.com/ipj>
- Training—Cisco offers world-class networking training. Current offerings in network training are listed at this URL:
<http://www.cisco.com/en/US/learning/index.html>

Document Change History

Table 5 describes the document changes made after the initial release of the *Cisco Media Gateway Controller Software Release 7 Operations, Maintenance, and Troubleshooting Guide*.

Table 5 **Summary History of Document Changes**

Subject	Document Number, Change Date	Change Summary
Operations Overview	OL-0542-04, March 30, 2001	Under “Element Management subsection” section, added the CIAgent and Cisco VSPT to the list.
Cisco MGC Operations	OL-0542-04, March 30, 2001	<p>Under “Managing Signaling Channels and Lines” section, added the “Managing Automatic Congestion Control” section, along with four related subsections.</p> <p>Under “Circuit Auditing” section, modified the Caution information on configuration library limitations.</p> <p>Under “Manual Switchover” section, modified the Caution information on configuration library limitations.</p> <p>Under “Config-Lib Viewer” section:</p> <ul style="list-style-type: none"> • modified the Note information on configuration library limitations. • indicated that the backup and restore functions are no longer valid as of 7.4(12).
Cisco MGC Operations	OL-0542-04, March 30, 2001	<p>Under “Setting Disk Space Utilization” section:</p> <ul style="list-style-type: none"> • modified the Note information on configuration library limitations. • rewrote section to more accurately define the disk monitor program.
Interpreting Report Files	OL-0542-04, March 30, 2001	Rewrote the “Configuring Log Files” section. Also added a recommendation to this section to ensure system functioning during times of high call volume.
Entire Document	OL-0542-05, August 2, 2001	<p>Imported latest documentation template.</p> <p>Removed all information specific to Release 7.3.</p>
Cisco MGC System Overview	OL-0542-05, August 2, 2001	<p>Changed the title of the chapter to more accurately reflect the content.</p> <p>Added Cisco MGC node description information from Troubleshooting Cisco MGC Node chapter.</p>

Table 5 Summary History of Document Changes (continued)

Subject	Document Number, Change Date	Change Summary
Cisco MGC Node Component Startup and Shutdown Procedures	OL-0542-05, August 2, 2001	<p>Changed the name of the chapter to more accurately reflect the content.</p> <p>Moved the “Starting MML” and “Managing Processes” sections to the Cisco MGC Node Operations chapter.</p> <p>Redefined the structure of the chapter.</p>
Cisco MGC Node Operations	OL-0542-05, August 2, 2001	<p>Changed the title of the chapter to more accurately reflect the content.</p> <p>Added a “Daily Operations” and regrouped existing procedures in it.</p> <p>Moved “Starting MML” and “Managing Processes” section over from the Starting and Stopping Software chapter.</p> <p>Modified the “Managing Automatic Congestion Control” section.</p> <p>Rewrote the “Setting Disk Utilization Levels” section, added the “Configuring Disk Monitor While the Software is Running” subsection.</p> <p>Updated all notes related to the 64 configurations limit to indicate that as of release 7.4(11), the number of configurations in the configuration library is automatically controlled using the disk monitor script.</p>
Cisco MGC Node Operations	OL-0542-05, August 2, 2001	<p>Moved field description information to the “Managing Traffic Channels” section from a similar section in the Troubleshooting the Cisco MGC Node chapter.</p> <p>Extensive additions, rewrites and links to content in other chapters.</p>
Troubleshooting the Cisco MGC Node	OL-0542-05, August 2, 2001	<p>Changed the title of the chapter to more accurately reflect the content.</p> <p>Removed the “Determining Traffic Channel States” section and referred to a similar section in the Cisco MGC Node Operations chapter.</p> <p>Added the “Alarm Troubleshooting Procedures” section which lists alarms that require corrective action.</p> <p>Extensive additions, rewrites, and links to content in the other chapters.</p>

Table 5 Summary History of Document Changes (continued)

Subject	Document Number, Change Date	Change Summary
Configuring Cisco MGC Report Files	OL-0542-05, August 2, 2001	Changed the title of the “Configuring the Log Files” to “Configuring the Data Dumper”. Added the “Configuring the Data Dumper to Support BAMS” section.
Troubleshooting Cisco SLT Signaling	OL-0542-05, August 2, 2001	Restructured content, reducing longer procedures to small modules.
Entire Document	OL-0542-05, August 15, 2001	Revised index markers throughout book.
Troubleshooting the Cisco MGC Node	OL-0542-05, August 15, 2001	Added the “Manually Resolving Stuck CICs” section.
Troubleshooting the Cisco MGC Node	OL-0542-05, October 1, 2001	Entered changes for 7.4(12), adding the following: <ul style="list-style-type: none"> Procedures for modifying MTP and RLM timers Procedure for enabling modification of properties.
Cisco MGC Node Operations	OL-0542-05, December 3, 2001	Updated field definitions for the rtrv-cic command. Updated chapter for timestamp changes. Added new backup procedures.
Troubleshooting the Cisco MGC Node	OL-0542-05, December 3, 2001	Updated chapter for timestamp changes. Added new restore procedures. Updated field definitions for the set-admin-state command.
Cisco MGC Node Operations	OL-0542-06, February 5, 2002	Added content on the new backup and restore viewers in the Cisco MGC toolbar. Modified ACC overload alarm descriptions.
Troubleshooting the Cisco MGC Node	OL-0542-06, February 5, 2002	Added new alarms. Added command descriptions to the <i>Viewing the Call Trace</i> section. Added the <i>Rebooting Software to Modify Configuration Parameters</i> section.
Configuring Cisco MGC Log Files	OL-0542-06, February 5, 2002	Updated the <i>Configuring the Data Dumper</i> Section. Added the <i>Understanding the Format of Log Files Archived Using Data Dumper</i> section.
Configuring Cisco MGC Log Files	OL-0542-06, February 12, 2002	Updated the <i>Configuring the Data Dumper</i> Section with a newly tested procedure.
Troubleshooting the Cisco MGC Node	OL-0542-06, February 20, 2002	Added a note to the Performing CIC Validation Tests Section indicating that these tests can only be performed on CICs associated with ANSI SS7-based DPCs. Modified the call stopping procedures to indicate that the confirm option must be used.

Table 5 Summary History of Document Changes (continued)

Subject	Document Number, Change Date	Change Summary
Cisco MGC Node Operations	OL-0542-06, June 26, 2002	<p>Updated state information for the rtrv-cic command.</p> <p>Updated backup operation section.</p> <p>Added a procedure to verify the amount of available virtual memory.</p> <p>Removed procedure for the rtrv-eqpt command.</p> <p>Adjusted range settings for the blk-cic command.</p>
Troubleshooting the Cisco MGC Node	OL-0542-06, June 26, 2002	<p>Updated descriptions of the commands to set the state of destinations and SPCs.</p> <p>Removed procedure for the set-eqpt-state command.</p> <p>Updated state information for the query-cic command.</p>
Configuring Cisco MGC Log Files	OL-0542-06, June 26, 2002	Clarified content to indicate that multiple CDBs can be created for each call.
Cisco MGC Node Operations	OL-0542-06, December 29, 2003	<p>Modified the <i>Backing up System Software</i> section with information regarding scheduling regular back-ups and removal of the .tar extension from the example backup files.</p> <p>Corrected default setting information for the <i>diskmonitor.SoftLimit</i> XECfgParm.dat parameter.</p> <p>Updated the <i>Verifying the Patch Level of the Cisco MGC</i> section, including information for the introduction of the Software Inventory Control functionality.</p>
Troubleshooting the Cisco MGC Node	OL-0542-06, December 29, 2003	Updated descriptions of the query-cic command indicating that it is not supported in all SS7 variants, and that it is able to support individual supervision messages.



Cisco MGC System Overview

This chapter provides an overview of the components of the Cisco Media Gateway Controller (MGC) node, and of the software architecture of the Cisco MGC software Release 7, which is used in both the Cisco SC2200 Signaling Controller and the Cisco PGW 2200 products.



Note

The Cisco PGW 2200 was formerly known as the Cisco VSC3000 Virtual Switch Controller. Some parts of this document may use this older name.

This information is described in the following sections:

- Cisco Media Gateway Controller Node, page 1-1
- Cisco MGC Software Architecture, page 1-3
- Cisco MGC Software Directory Structure, page 1-10

Cisco Media Gateway Controller Node

The following subsections briefly describe the components of the Cisco MGC node:

- Cisco Media Gateway Controller, page 1-1
- Cisco Signaling Link Terminals, page 1-2
- Cisco Catalyst 5500 Multiswitch Routers, page 1-2

The Cisco MGC Node Manager (CMNM) and Billing and Measurements Server (BAMS) are optional components of the Cisco MGC node that are not dealt with in this document. For more information on the CMNM, refer to the *Cisco Media Gateway Controller Node Manager User's Guide*. For more information on the BAMS, refer to the *Billing and Measurements Server User's Guide*.

Cisco Media Gateway Controller

The Cisco MGC is a Sun Netra UNIX host running Cisco MGC software Release 7. The Cisco MGC performs real-time call-processing and SS7 layer functions; manages trunk resources, alarms, and call routing; and administers billing information.

Cisco MGC functionality includes:

- Processing calls
- Originating call detail records (CDRs)

- Providing alarm initiation information
- Producing operational peg counts
- Receiving and processing craft user interface (CUI) data
- Providing Message Transfer Part (MTP) Level 3 (MTP3) functions
- Providing advanced intelligent network (AIN) capabilities

Sun Netra Hosts

Sun Netra UNIX hosts serve as the platform for the Cisco MGC software Release 7. The Sun Netra hosts meet or exceed Network Equipment Building System (NEBS) Level 3 standards.

Using two Sun Netra UNIX hosts in a continuous service configuration provides system redundancy and reliability. The call-processing application is active on one Cisco MGC and switches to the standby Cisco MGC only under failure conditions.

Cisco Signaling Link Terminals

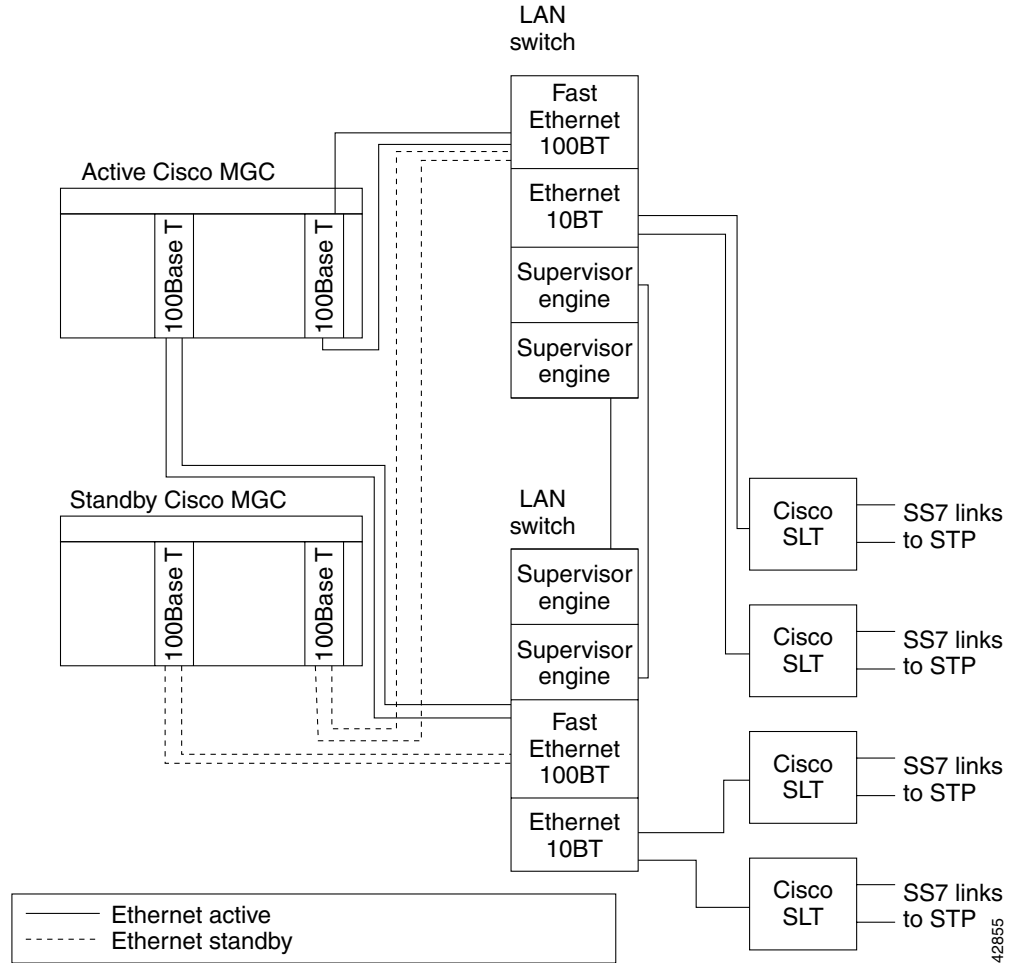
The Cisco Signaling Link Terminals (SLTs) terminate SS7 links. Each Cisco SLT supports up to two signaling network connections. Multiple Cisco SLTs (up to 16 per Cisco MGC node) can be used to support additional signaling channels or provide redundant signal paths between the signaling network and the control signaling network. The Cisco SLTs support V.35, T1 and E1 interfaces to the SS7 network. Each interface card supports a single DS0 signaling channel. MTP Level 1 (MTP1) and MTP Level 2 (MTP2) are terminated at the Cisco SLTs and the remaining SS7/C7 layers are backhauled, using the Reliable User Datagram Protocol (RUDP), over a 10BASE-T Ethernet interface across the IP network to the Cisco MGC host.

Cisco Catalyst 5500 Multiswitch Routers

The Cisco Catalyst 5500 multiswitch routers are local area network (LAN) switches that are used to create the Ethernet backbone between the Cisco MGCs, Cisco SLTs, and Cisco media gateways. The Cisco Catalyst 5500 is the recommended LAN switch for the Cisco MGC node.

Ethernet Connections

Each Ethernet NIC for each Cisco MGC is connected by a 100BASE-T interface to the LAN switches. The LAN switches connect to the Cisco SLTs using 10BASE-T interfaces. Figure 1-1 displays the Ethernet connections between the elements of the Cisco MGC node.

Figure 1-1 Cisco MGC Node Connectivity

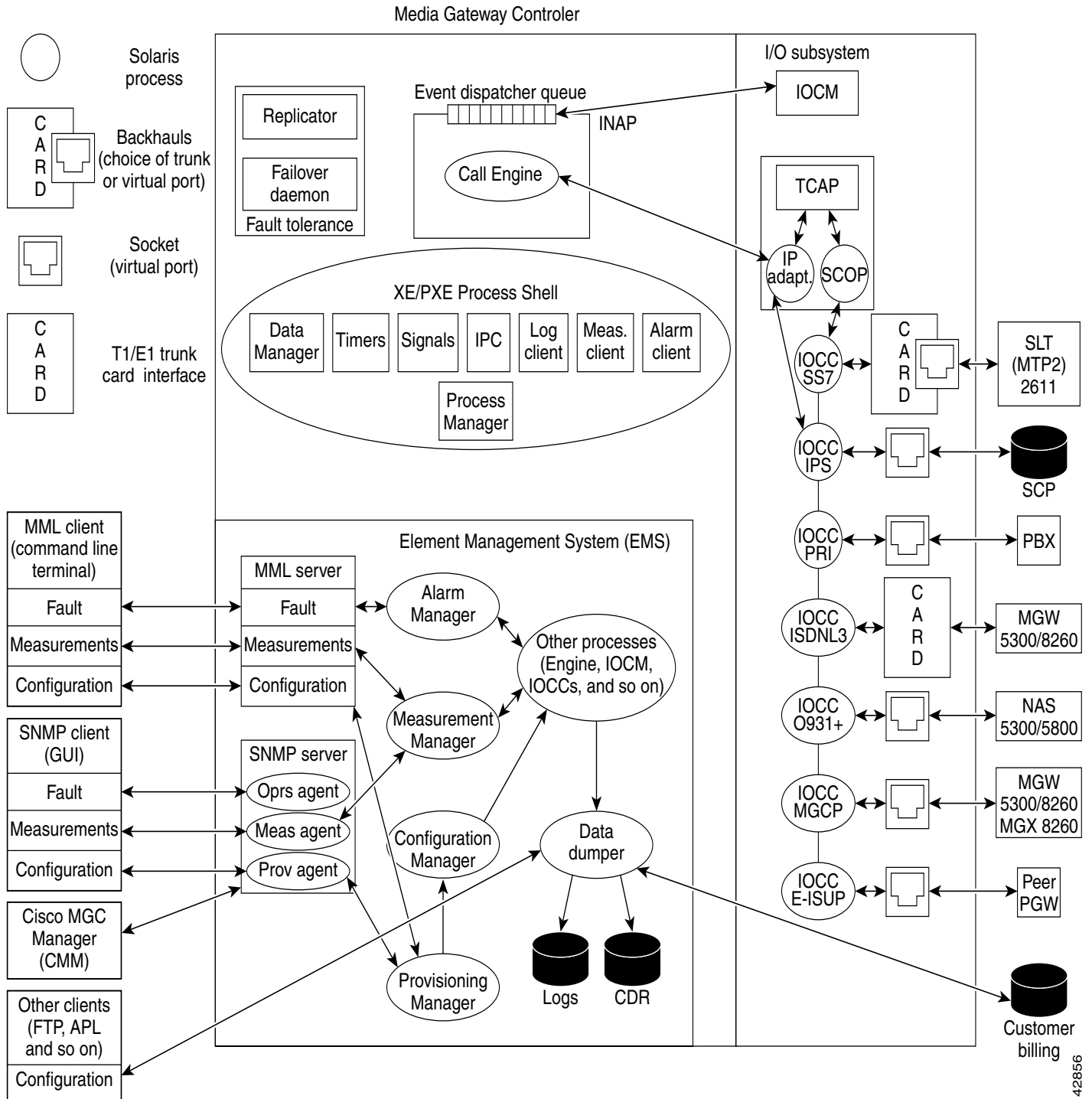
42855

Cisco MGC Software Architecture

This section describes the major subsystems in the Cisco MGC software, which are illustrated in Figure 1-2. The major subsystems are

- Input/Output Subsystem, page 1-5
- Element Management Subsystem, page 1-5
- Fault Tolerance Subsystem, page 1-6
- Execution Environment Process Shell, page 1-7
- Call Engine Process, page 1-8

Figure 1-2 Cisco MGC Software System Diagram



Input/Output Subsystem

The Input/Output (I/O) subsystem consists of the I/O channel controllers (IOCC) and the I/O channel manager (IOCM), which manages them.

- The IOCM manages all IOCCs and keeps the hardware resource states of the hardware controlled by the IOCCs.
- The IOCCs provide
 - A protocol-specific, message-based interface that allows nodes and platforms external to the Cisco MGC to communicate with the Cisco MGC.
 - An interface that allows buffering of messages to the call engine's event dispatcher queue.
- The Cisco MGC I/O subsystem includes the following IOCCs:
 - Internet protocol services (IPS)—Designed to migrate Transaction Capabilities Application Part (TCAP) on top of TCP/IP for connecting to Signal Transfer Points (STPs) and Service Control Points (SCPs) for intelligent network (IN) services.
 - Signaling System 7 (SS7)—Contains MTP3 used for backhauling SS7 signaling to the Cisco MGC from a Cisco SLT.
 - Primary Rate Interface (PRI)—Supports ISDN termination to a private branch exchange (PBX).
 - ISDN Level 3—Provides backhauling of ISDN (standard variants) to the Cisco MGC from a media gateway.
 - Q931+—Is a stateless IOCC, a special version of ISDN that enables forwardhauling of Q931+ signaling to a media gateway used in Cisco SC2200 environments.
 - Media Gateway Control Protocol (MGCP)—Enables communication to media gateways and trunking gateways for setting up bearer channel connections used in Cisco PGW 2200 environments.
 - Extended ISDN User Part (E-ISUP)—Cisco-proprietary internal interface that enables the transport of endpoint and media gateway specific information between two (or more) Cisco MGCs. This protocol uses an enhanced ISUP base to support all ANSI and ITU ISUP messaging and elements, as well as additional fields to support transport of service information (such as local number portability (LNP), 800 numbers, and so on).

Element Management Subsystem

The Element management subsystem (EMS) allows external client software or terminals to gain access to the data in the Cisco MGC. The functions this subsystem supports are:

- Configuration management—Adding, deleting, or modifying parameters and resources needed by the Cisco MGC to perform its switching function. This data is stored locally in data (.dat) files. This data is required to automate reconfiguration after a process failure.
- Alarm management—Reporting and clearing alarms generated by Cisco MGC processes.
- Performance measurement management—Reporting and clearing metrics generated by Cisco MGC processes. You can also define thresholds which, if exceeded, could produce alarms.
- Accounting management—Dumping generated call detail records (CDRs) to locally persistent files or to remote databases through a standard or customized API.

The following types of external clients can access or manipulate data on the Cisco MGC:

- **Man-Machine Language (MML) terminal**—Serves as a command-line interpreter where a craftsperson can manipulate data for fault detection, measurements, or configuration through a series of commands. MML is similar to TL/1 and is best suited for low-level system experts (such as operations personnel) for rapid system configuration or troubleshooting.
- **SNMP-Based Terminal**—Any client using SNMP, usually a craftsperson with a graphical user interface (GUI) application, can access data for fault reporting, measurements, configuration, or security. SNMP applications are best suited for end users and allow development of elaborate multiplatform client applications to satisfy diverse customer needs.

Starting with Release 7.4(11), the Cisco MGC uses a master agent, EMANATE from SNMP Research, and related subagents to enable SNMP access to the system. The Cisco MGC uses the following subagents:

**Note**

Refer to the *Release Notes for the Cisco Media Gateway Controller Software Release 7.4(11)* for more information.

- **Operations**—A custom subagent that provides access to fault data
- **Measurement**—A custom subagent that provides access to measurement data
- **Critical application monitor**—A standard CIAgent subagent that is used to monitor the process manager process
- **Host resources MIB**—A standard CIAgent subagent that is used to access data, such as the number of processors, and memory usage on the Cisco MGC host platform
- **MIB-II**—A standard CIAgent subagent that partially supports the MIB-II standard (RFC-1213)
- **File system monitor**—A standard CIAgent subagent that monitors thresholds for five file systems
- **Cisco MGC Manager (CMM)**—Is an application used for provisioning the Cisco MGC.
- **Cisco Voice Service Provisioning Tool (VSPT)**—As of Release 7.4(11), this application can be used for provisioning the Cisco MGC. Refer to the *Release Notes for the Cisco Media Gateway Controller Software Release 7.4(11)* for more information.
- **Cisco MGC Node Manager (CMNM)**—Is an optional application used for network element (NE) management.

Fault Tolerance Subsystem

The goal of the fault tolerance subsystem is to ensure call preservation if the Cisco MGC encounters a fault condition. There are two processes that ensure this:

- **Failover daemon**—Monitors Cisco MGC processes using a heartbeat mechanism. If there is no response to its process polling in a fault-tolerant hardware configuration, the Cisco MGC switches control to the standby unit.
- **Replicator**—Allows processes to checkpoint critical call information, such as signaling and bearer states, as well as call data across the active and standby processors. Its goal is to replicate enough information for established calls to survive a failover. Checkpointing events are generated at two points in a call:
 - When the call is answered, to update the full duplex path.

- When the call is released, after the physical resources are deallocated.

Connectionless (non-call) signaling may be generated by a craftsperson performing maintenance through an MML or SNMP client or by circuit supervision.

Certain signaling can also generate checkpointing events:

- Blocking or unblocking of circuits
- Circuit reset

**Note**

The replicator mechanism does not try to replicate program or data storage. Service features are not checkpointed across processors; there is just enough information to maintain the voice or data path between the call originator and the call terminator.

If the switchover happens before the simplex path is established, call processing cannot proceed on the inactive side. Non-established calls in the process of being set up are lost.

Execution Environment Process Shell

The execution environment provides an operating system process shell used by Cisco MGC processes to access lower-level functionality. Such functionality holds together the I/O, element management, and call engine subsystems in the Cisco MGC. The execution environment infrastructure provides the following functions to Cisco MGC processes:

- Operating system interface—Such as the Sun Solaris operating system.
- Process management—Performs startup order, shutdown order, and monitoring of processes. Also performs software upgrade compatibility checking with minimal service interruption.
- Alarm management—Allows processes to register, set, and clear alarms, which are then presented to the EMS for further processing.
- Log management—Allows MGC processes to log messages to locally persistent data files. Message codes (instead of strings) minimize the overhead of interprocess transport of long buffers. Log files use a facility (process type originating the log) and a logging level (severity).
- Measurement management—Allows processes to adjust counters or other metrics, which are subsequently presented to the EMS for Alarm and Measurement Report processing.
- Command management—An interface that can be used by any active processes or by an EMS interface, such as MML or SNMP agents, to exchange commands or responses.
- Configuration management—Notifies processes and gets responses when configuration data changes. Handles reconfiguration management when multiple processes are affected by changes.
- Access control—Allows only authorized processes to access certain services or other processes.
- Interprocess communication (IPC)—Allows processes to exchange messages.
- Event Processing Service—The XEProcShell facility allows applications to register, deregister, and exchange events (messages) through IPC. This service is critical to efficient real-time CPU usage and overall system performance.
- Timers—Allow processes to set, clear, or monitor timers. Provide timeouts to processes.

Call Engine Process

The call engine is a process designed to provide the means and resources for call processing to take place. The call engine involves the following components:

- Resource manager—Performs the following functions:
 - Tracks all bearer resources used. Proxies and tracks the bearer resources in the trunking gateways within the Cisco MGC's service area.
 - Services all requests for allocation or deallocation of bearer resources from call instances.
 - Executes bearer allocation algorithms (circuit selection).
 - Manages echo cancellation on the call's behalf.
 - Performs continuity tests.
 - Checkpoints bearer states and modes to the standby Cisco MGC to guarantee that the bearer channel is not lost during a manual or automatic switchover.
- Connection manager—Interfaces with the nodes and protocols external to the Cisco MGC that are necessary to establish an IP (TCP, UDP, or RUDP) or PSTN connection that is managed by the Cisco MGC. The type of node supported is
 - VoIP/VoATM trunking gateways using MGCP.
 - Time Domain Multiplex (TDM) trunking gateways using MGCP.
- Call manager—Contains and selects the appropriate protocol adapters. These are protocol-specific entities performing the following functions:
 - Communicates with the corresponding protocol-specific IOCC.
 - Converts incoming protocol data units (PDUs) received from the IOCC to an internal, protocol independent format.
 - Converts internal, protocol-independent PDUs to protocol-specific format.
 - Communicates current circuit states to the IOCM using the IOCCs.
 - Creates a call instance when an incoming MTP3 call establishment message is received.
 - Destroys that instance and frees any associated memory when the call is terminated.
 - Supports multiple call instances. It dequeues incoming messages from the event dispatcher queue and routes them to the call instance for which they are destined.
 - Generates call detail blocks (CDBs), which are used to create CDRs.
 - Operates as a standby entity, which is created when the call engine is created at system startup, and waits to create a new call, destroy an existing call, or process an event for an existing call.
 - Checkpoints call information, such as call signaling state and data, to the standby Cisco MGC to guarantee that the signaling link is not lost during a manual or automatic switchover.

Call Instance Component

A call instance is the dynamic component of the Cisco MGC that is created at run time and is the place where call processing takes place. The call instance is commonly referred to as the Message Definition Language (MDL) component, which is the language used to implement it.

A call is instantiated when an incoming MTP3 call establishment message is received. There is always a one-to-one relationship between a call instance and a call switched by the Cisco MGC.

There are several significant subcomponents involved in a call instance:

- Originating call control (OCC)—Is the instance of the originating protocol's state machine. In defining a protocol, two MDL modules are created:
 - A general declarations module, which contains protocol-specific types and definitions.
 - A protocol definition module, which contains the state logic for two state machines—one for call origination and one for call termination. This module produces an object file named *protocolName.mdo*.
- Universal call model (UCM)—Is a protocol-independent state machine that is used to
 - Provide protocol interworking between the originating and the terminating sides of the call.
 - A UCM MDL module is used to define the UCM behavior and logic. The UCM module is compiled into an object file, but can only be loaded by the Call Engine and cannot be used by any of the protocols.
 - Provide event-driven logic, which controls the following call-processing functions: linking the OCC and the terminating call control (TCC), updating and retrieving the call context structures, interacting with other call engine components, such as the resource manager, connection manager, and call manager, managing bearer resources, such as trunking gateways, using the MGCP, and keeping the call processing state machine.
 - The UCM also triggers events to be processed by the following MDL modules: generic analysis module, subscriber profile retrieval, a-number and b-number pre-analysis, a-number and b-number full analysis, route selection, and the IN trigger module.
- Connection plane manager (CPM)—Communicates with the call engine's resource manager to make the bearer connections to a remote trunking gateway using MGCP.
- CDR Manager—Generates CDRs and forwards them to the EMS to be locally persisted or forwarded for off-platform accounting applications. CDRs are generated when calls are answered and they can also be generated in the following situations:
 - End of call (standard)
 - Long duration calls
 - Mid-call CDRs (can generate CDBs at eight different points in a call)
- Terminating call control—Is the instance of the terminating protocol's state machine.
- Call context—The following are the call context characteristics:
 - A persistent object in a call instance that serves as the placeholder for bearer and signaling information. Such information is set and retrieved by the OCC, TCC, or UCM at various points in the life of the call.
 - An MDL context definition module is used to define the information elements, structures, and fields. This module is compiled into an object file to be used by all protocols.

The format of these structures is protocol-independent to minimize cross-protocol conversion permutations. Contains rules for data conversion to and from each protocol.
 - Collects the following call information in CDBs, which are assembled to build CDRs: calling number, called number, answer time, disconnect time, originating trunk group and circuit identification code (CIC), terminating trunk group and CIC, address translation and route information, ISUP information, ISDN service information, database query information, call completion codes, and other information depending on the type of call.

Cisco MGC Software Directory Structure

This section shows an overview of the UNIX file directory tree for the Cisco MGC distribution, along with a brief description of the purpose for each directory. This section is to be used as a guide to finding files called out in the operational procedures.

In the installation procedures, the installer is asked for a directory under which to install the Cisco MGC software. The default directory is /opt/CiscoMGC; however, this directory name is installer-definable, so do not assume that /opt/CiscoMGC is always used. This is the directory under which all files for the Cisco MGC reside. The sole exception is some temporary files that are created at run time.

Table 1-1 utilizes the variable \$BASEDIR to indicate the directory into which the Cisco MGC software was installed.

Table 1-1 Cisco MGC Software Directory Structure

Directory	Description
\$BASEDIR/bin	Cisco MGC executable programs that cannot be customized.
\$BASEDIR/local	Cisco MGC executable programs that can be modified by the customer for a site-specific reason. See the procedures for how to customize files. Generally the factory default values are sufficient.
\$BASEDIR/etc	Network element configuration files. This includes all provisionable configuration files required for proper operation of the Cisco MGC.
\$BASEDIR/etc/CONFIG_LIB	Cisco MGC configuration file library. This is a simple version control system for configuration file changes.
\$BASEDIR/etc/cust_specific/toolkit	Saved data from the Cisco MGC Toolkit applications is stored in this directory.
\$BASEDIR/lib	Shared object files. These libraries are loaded at runtime by the executables. The three types of libraries are: (1) system/program shared objects, (2) MDL interpreted objects, and (3) MDL shared objects.
\$BASEDIR/var	Subsystem communication and persistent storage area. This directory contains files and devices providing communications between the various subsystems in the Cisco MGC. It also contains files providing persistent storage of data for the Cisco MGC.
\$BASEDIR/var/log	System logging area. This directory contains the platform logs. See the “Recovering from a Switchover Failure” section on page 8-113 for more information.
\$BASEDIR/var/spool	Dumper Spool Area. This directory contains historic reports. See Appendix A, “Configuring Cisco MGC Report Files.”
\$BASEDIR/var/trace	Signal Path Trace area. This directory contains all MDL trace logs used for conversion analysis.
\$BASEDIR/data	MDL source files. MDL source files are generally not provided, but if they are purchased, they will appear here.



Cisco MGC Node Component Startup and Shutdown Procedures

This chapter describes the steps necessary to startup and shutdown the individual components of the Cisco Media Gateway Controller (MGC) node.

The startup procedures for each component of the Cisco MGC node are included in the following sections:

- Cisco Media Gateway Controller Startup Procedures, page 2-1
- Cisco Signaling Link Terminal Startup Procedure, page 2-3
- Cisco Catalyst 5500 Multiswitch Router Startup Procedure, page 2-3

You might need to perform these tasks if you:

- Have made changes to the system configuration
- Are upgrading the software
- Are testing the system
- Are troubleshooting alarms
- Are trying to resolve a problem



Note

In these procedures, it is assumed that the component has been correctly installed, configured, and provisioned in accordance with the instructions provided in the relevant documentation.

Shutdown procedures for each component of the Cisco MGC node are included in the following sections:

- Cisco Media Gateway Controller Shutdown Procedure, page 2-4
- Cisco Signaling Link Terminal Shutdown Procedure, page 2-5
- Cisco Catalyst 5500 Multiswitch Router Shutdown Procedure, page 2-5

Cisco Media Gateway Controller Startup Procedures

This section contains the hardware and software startup procedures for the Cisco MGC.

Starting the Cisco MGC Hardware

The system switch of the Cisco MGC is a rocker, momentary contact switch that functions as a standby device only, controlling the logic circuits that enable power module output.

To power on the system, complete the following steps:

-
- Step 1** Turn on the power to all connected peripherals.



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

- Step 2** Apply power to the system inlet.

- Step 3** Press the front panel ON/STBY system switch to the ON position and hold it until the system starts to power up.
-

Starting the Cisco MGC Software

Under normal conditions, simply powering up the system automatically launches the Cisco MGC software and the Simple Network Management Protocol (SNMP) daemon using system defaults. See the “Configuring SNMP” section in the *Cisco Media Gateway Controller Software Release 7 Installation and Configuration Guide* for more information about SNMP.



Note In this section, it is assumed that the Cisco MGC software Release 7 has been correctly installed, configured, and provisioned on the host server and that you have the appropriate packages, or applications, for your system. If the Cisco MGC Release 7 software has been installed, configured, or provisioned incorrectly, or if you are having other problems, see Chapter 8, “Troubleshooting the Cisco MGC Node,” for more information.



Note To perform the procedures in this section, you must have a user ID that is part of the Cisco MGC group (mgcgrp) and you must have the proper group privileges. To verify that your user ID is part of the Cisco MGC group and that you have the necessary privileges, refer to the “Configuring Groups and Users” section in the *Cisco Media Gateway Controller Software Release 7 Installation and Configuration Guide* for more information.

Starting up the Cisco MGC software manually



Caution Do not use the following commands unless specifically instructed to do so by Cisco Technical Assistance Center (TAC) personnel.

To manually start the Cisco MGC software, log in to the active Cisco MGC as root and enter the following command:

```
/etc/init.d/CiscoMGC start
```

This action restores execution permission and enables the automated startup script.

Cisco Signaling Link Terminal Startup Procedure

This section contains the recommended startup procedure for the Cisco Signaling Link Terminal (SLT).

**Note**

In this section, it is assumed that the Cisco SLT has been correctly installed and configured and that the correct software version is installed. If you are experiencing problems, see Appendix B, “Troubleshooting Cisco SLT Signaling,” for detailed information.

To start up a Cisco SLT, perform the following steps:

-
- Step 1** Before you start the Cisco SLT, verify the following:
- All modules are installed correctly, and all interface cable connections are secure.
 - The power cable is connected to both the rear panel power connector and the power source.
 - A terminal is connected to the console port and is turned on.
- Step 2** Turn the power on (I). During the boot process, observe the following:
- The power LED on the front panel should be green.
 - You should hear the system fans operating.
 - The console terminal displays a script and system banner.
- Step 3** Press Return at the Enter Password prompt to access the console command line.
-

Cisco Catalyst 5500 Multiswitch Router Startup Procedure

This section contains the recommended startup procedure for the Cisco Catalyst 5500 LAN switches.

**Note**

In this section, it is assumed that the Cisco Catalyst 5500 LAN switch has been correctly installed and configured and that the correct software version is installed. If you are experiencing problems, see Appendix C, “Troubleshooting Cisco Catalyst 5500 Multiswitch Routers Signaling,” for detailed information.

To start the Cisco Catalyst 5500 LAN switch, complete the following steps:

-
- Step 1** Before you start the Cisco Catalyst 5500 LAN switch, verify the following:
- All modules are installed correctly, and all interface cable connections are secure.
 - Each power supply is installed correctly and is connected to a grounded power source.
 - If two power supplies are present, each power cord is connected to a different line.
 - A terminal is connected to the supervisor module console port and is turned on.
- Step 2** Turn the power supplies on (I). During the boot process, observe the following:

- The LEDs on the power supplies should be green.
- The PS1, PS2, and fan LEDs on the supervisor engine should be green, and you should hear the system fans operating.
- The System Status LED on the supervisor engine should be green after the boot is complete. It flashes red, orange, and green during startup.
- The supervisor engine interface LEDs and module LEDs (such as the Link LEDs) might blink or stay lit continuously during the boot process. Many module LEDs do not go on until you configure the interfaces. Wait until the boot is complete before trying to verify the module LED indications.
- The console terminal displays a script and system banner.
- The supervisor engine begins to initialize the modules once the boot process is completed. Messages appear on the console as the modules come online.

Step 3 Press Return at the Enter Password prompt to access the console command line.

Cisco Media Gateway Controller Shutdown Procedure

This section contains the software and hardware shutdown procedures for the Cisco MGC.

Shutting Down the Cisco MGC Software Manually



Caution

Do not use the following commands unless specifically instructed to do so by Cisco Technical Assistance Center (TAC) personnel.

To manually stop the Cisco MGC software, log into your active Cisco MGC as root and enter the following command:

```
/etc/init.d/CiscoMGC stop
```

This action disables the automated startup script.

Shutting Down the Cisco MGC Hardware

To shut down the Cisco MGC, you remove power from the system. The power switch of the Cisco MGC is a rocker, a momentary contact switch that functions as a standby device only, controlling logic circuits that enable power module output.



Caution

Before you turn off the power, exit from the operating system. Failure to do so might result in data loss.

To shut down the Cisco MGC, complete the following steps:

Step 1 Where necessary, notify users that the Cisco MGC is going down.

Step 2 Back up system files and data prior to shutdown. Refer to the “Backing Up System Software” section on page 3-28.

- Step 3** Exit from the operating system. Refer to your Sun documentation for the appropriate commands to be used to exit from the operating system.



Note Ensure that you use the UNIX command **init 5** as part of exiting from the operating system. This command is described in the Sun documentation.

- Step 4** Momentarily set the front panel power switch to the STBY position until the system powers down.
- Step 5** Verify that the POWER LED is off.
- Step 6** Remove the input power connector from the power inlet.



Caution Regardless of the position of the ON/STBY switch, where an AC or DC power cord remains connected to the system, voltage may be present within the power supply.

Cisco Signaling Link Terminal Shutdown Procedure

To shut down the Cisco SLTs, simply set the power switches to the OFF (0) position.

When the power switches are in the OFF (0) position, the power LEDs on the front panels should be off and the fans should not be operating.

Cisco Catalyst 5500 Multiswitch Router Shutdown Procedure

To shut down the Cisco Catalyst 5500 MSR, simply set the power switches to the OFF (0) position.

When the power switches are in the OFF (0) position, the LEDs on the power supplies should be off and the fan assembly should not be operating.



Cisco MGC Node Operations

This chapter contains recommended operating procedures for the Cisco Media Gateway Controller (MGC) node. In these procedures, the assumption is that all components have been correctly installed, configured, and provisioned in accordance with the instructions provided in the relevant documentation. All components are assumed to have been successfully started, as described in Chapter 2, “Cisco MGC Node Component Startup and Shutdown Procedures.”



Note

Operation of the Cisco MGC node should be performed by someone who has been trained in the complexities of the system, who has some experience administering the system, and who understands UNIX at the system administrator level.

This chapter contains the following sections:

- Daily Tasks, page 3-1
- Periodic Maintenance Procedures, page 3-23
- Regular Operations, page 3-39

Daily Tasks

The following section detail the procedures you should perform on a daily basis on the Cisco MGC. These procedures use Man-Machine Language (MML) and UNIX commands. These procedures can also be performed using the optional Cisco MGC Node Manager (CMNM) application. For more information on using the CMNM to operate the Cisco MGC, refer to the *Cisco MGC Node Manager User's Guide*.

The tasks you should perform on a daily basis are found in the following sections:

- Starting an MML Session, page 3-2
- Verifying the Platform State of the Cisco MGC Hosts, page 3-2
- Verifying That Processes Are Running, page 3-3
- Monitoring the Alarms Status, page 3-6
- Verifying the Status of all Destinations, page 3-8
- Verifying State of all SS7 Routes, page 3-10
- Verifying CIC States, page 3-13
- Verifying Available Disk Space, page 3-17
- Verifying Available Virtual Memory, page 3-17

- Verifying Available RAM, page 3-19
- Verifying CPU Utilization Level, page 3-19
- Verifying the Number of Active Processes, page 3-21
- Verifying the Number of Users, page 3-22
- Verifying Available Memory on the Cisco SLTs, page 3-23

Starting an MML Session

When a procedure requires that you start an MML session, you must perform the following steps:



Note

We recommend that you run your MML sessions from the active Cisco MGC, unless the procedure indicates otherwise.

Step 1 Log in to the active Cisco MGC.

Step 2 Enter the following command at the UNIX prompt:

```
mml
```

If you receive an error message indicating that sessions are already in use, enter the following command:

```
mml -s session number
```

Use any session number from 2 through 12 and repeat until you find a vacant session. Once you have successfully started an MML session, the prompt changes to:

```
machine_name mml>
```

Verifying the Platform State of the Cisco MGC Hosts

You can determine which of your Cisco MGC hosts is the active Cisco MGC and which is the standby Cisco MGC. If your system uses a Cisco MGC in a simplex configuration, the single Cisco MGC host is always active. To do this, complete the following steps:

Step 1 Log into one of the Cisco MGCs, 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 Cisco MGC:

```
Media Gateway Controller 2000-03-29 14:15:22
M RTRV
"Type:MGC"
"Hardware platform:sun4u sparc SUNW,Ultra-5_10"
"Vendor:"Cisco Systems, Inc.""
"Location:Media Gateway 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 Cisco MGC, 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 either the active or standby platform state.

If the Cisco MGC hosts have changed their platform state, determine why the switchover occurred by searching the contents of the active system log file, as described in the “Viewing System Logs” section on page 8-4.

If the platform state of either Cisco MGC host is OOS, check the alarms as described in the “Monitoring the Alarms Status” section on page 3-6, and take the actions necessary to correct the condition that caused the associated alarm(s). The alarms that require you to take corrective action and their associated actions can be found in the “Alarm Troubleshooting Procedures” section on page 8-8. A complete listing of alarms can be found in the *Cisco Media Gateway Controller Software Release 7 Messages Reference Guide*.

If the platform state of both Cisco MGC hosts is active, proceed to Step 4.

- Step 3** Verify that the active configuration has not changed by entering the following UNIX commands:

```
cd /opt/CiscoMGC/etc
ls -l
```

The system returns a response similar to the following:

```
total 35350
-rw-r--r-- 1 mgcusr mgcgrp 38240 May 8 10:46 02.trigger
-rw-rw-r-- 1 mgcusr mgcgrp 20488 Oct 10 2000 64eisup.bat
lrwxrwxrwx 1 mgcusr mgcgrp 43 Aug 1 18:55 active_link ->
/opt/CiscoMGC/etc/CONFIG_LIB/CFG_pol-addipl
-rw-rw-rw- 1 mgcusr mgcgrp 30907 Jul 24 15:29 alarmCats.dat
-rw-rw-rw- 1 mgcusr mgcgrp 2064 Jun 4 10:57 alarmTable.dat
-rw-rw-rw- 1 mgcusr mgcgrp 0 Jun 4 10:57 auxSigPath.dat
```

Identify the active_link file. The listing indicates which configuration is currently active. The active configuration in the example is CFG_pol-addipl.

If the configuration has changed, you may want to compare the active configuration to the previous configuration.

- Step 4** 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 That Processes Are Running

To verify that the processes on your Cisco MGC are running, perform the following steps:

- Step 1** Log in to the active Cisco MGC, start an MML session, and enter the following command:

```
rtrv-softw:all
```

The system returns a response similar to the following:

```
Media Gateway Controller - MGC-04 2000-04-05 08:06:03
M   RTRV
    "CFM-01:RUNNING ACTIVE"
    "ALM-01:RUNNING ACTIVE"
    "MM-01:RUNNING ACTIVE"
    "AMDMPR-01:RUNNING ACTIVE"
    "CDRDMPR-01:RUNNING ACTIVE"
    "DSKM-01:RUNNING IN N/A STATE"
    "MMDB-01:RUNNING IN N/A STATE"
    "POM-01:RUNNING ACTIVE"
    "MEASAGT:RUNNING ACTIVE"
    "OPERSAGT:RUNNING ACTIVE"
    "PROVSAGT:RUNNING ACTIVE"
    "MGCP-1:RUNNING IN N/A STATE"
    "Replic-01:RUNNING ACTIVE"
    "ENG-01:RUNNING ACTIVE"
    "IOCM-01:RUNNING ACTIVE"
    "TCAP-01:RUNNING IN N/A STATE"
    "FOD-01:RUNNING IN N/A STATE"
    "EISUP-1:RUNNING IN N/A STATE"
    "SS7-A-1:RUNNING IN N/A STATE"
```



Note

If this MML command is entered on the standby Cisco MGC, the state of the processes is either **RUNNING STANDBY** or **RUNNING IN N/A STATE**.

Step 2 If any of the processes are initializing, wait a few moments and repeat Step 1. If that process is still initializing, contact the Cisco TAC for assistance. Refer to the “Obtaining Technical Assistance” section on page xviii for more information on contacting the Cisco TAC.

If any of the processes are stopped, contact the Cisco TAC for assistance. Refer to the “Obtaining Technical Assistance” section on page xviii for more information on contacting the Cisco TAC.

Understanding Processes

The Cisco MGC software contains processes and process groups that perform various functions. These functions include managing the I/O channels; generating alarms, call detail records (CDRs), and logs; and performing signal conversion. All these processes are managed by the process manager process of the Cisco MGC software.

Three different monitoring levels are offered:

- Active process—Controlled and monitored directly by the process manager.
- Passive process—Does not communicate with the process manager.
- Monitoring process—Periodically runs an executable or script and sets or clears an alarm based on the return code. This type of process can monitor other processes or tasks that can be checked programmatically. Some examples are the amount of available disk space, system daemon existence, and established process dependency.

Table 3-1 shows the system processes and process groups controlled by the process manager.

Table 3-1 Processes Controlled by the Process Manager

Group	Process	Description
ENGG-01		Engine Group
	Replic-01	Replicator controller. It is an active process. If it should go down, it causes a critical out-of-service alarm.
	ENG-01	Call engine. It is an active process. If it should go down, the system cannot process calls. Its failure causes a critical out-of-service alarm.
IOSG-01		I/O Subsystem Group
	IOCC-01	I/O channel controller. It is a passive process. If it should go down, it causes a critical out-of-service alarm.
	IOCC-02	I/O channel controller. It is a passive process. If it should go down, it causes a critical out-of-service alarm.
	IOCM-01	I/O channel manager. It is a passive process. If it should go down, it causes a major out-of-service alarm.
	TCAP-01	TCAP and SCCP protocol handler. It is a passive process. If it should go down, it causes a major out-of-service alarm.
XEG-01		Execution Environment Group
	CFM-01	Configuration manager. It is an active process. If it should go down, it causes a major out-of-service alarm.
	ALM-01	Alarm manager. It is an active process. If it should go down, it causes a major out-of-service alarm.
	AMDMPR-01	Alarm and measurement dumper. It is an active process. If it should go down, it causes a major out-of-service alarm.
	MM-01	Measurement manager. It is an active process. If it should go down, it causes a major out-of-service alarm.
	CDRDMPR-01	CDR dumper. It is an active process. If it should go down, it causes a major out-of-service alarm.
	MMDB-01	TimesTen database. It is a passive process. If it should go down, it causes a minor out-of-service alarm.
FTG-01	POM-01	Provisioning object manager. It is an active process. If it should go down, it causes a major out-of-service alarm.
		Failover Group
	FOD-01	Failover controller. It is a monitoring process. If it should go down, it causes a minor out-of-service alarm.
PFMG-01		Platform Monitoring Group
	DSKM-01	Disk space monitor. This shell script monitors disk space and trims back older files in case the current amount of free space is below a specified threshold. This is a monitoring process. If it should go down, it causes a minor out-of-service alarm.

Table 3-1 Processes Controlled by the Process Manager (continued)

Group	Process	Description
SNMPG-01		SNMP Group
	MEASAGT	Measurements SNMP agent. This is an active process. If it should go down, this is a major out-of-service alarm.
	PROVSAGT	Provisioning SNMP Agent. This is an active process. If it should go down, this is a major out-of-service alarm.
	OPERSAGT	Operational SNMP Agent. This is an active process. If it should go down, this is a major out-of-service alarm.

Monitoring the Alarms Status

If you monitor the alarm status of the Cisco MGC continuously, you can determine how often a particular alarm occurs in a specific period of time. To monitor the alarm status of the Cisco MGC on a continuous basis, perform the following steps:

Step 1 Log in to the active Cisco MGC, start an MML session, and enter the following command:

```
rtrv-alm::cont
```

The system returns a response that shows all active alarms:

```
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"
```

Step 2 If an alarm appears, you can determine the appropriate course of action by referring to the listing for that alarm in the *Cisco Media Gateway Controller Software Release 7 Messages Reference Guide*. Detailed descriptions of the actions required to resolve the problems associated with the alarm are found in Chapter 8, “Troubleshooting the Cisco MGC Node.”

You can also find additional information on the conditions that caused the alarms by viewing the system logs. The logs can be viewed using the log viewer, part of the Cisco MGC viewer toolkit. For information on using the log viewer, see the “Using the Log Viewer” section on page 3-114.

**Note**

Once you have begun monitoring alarms continuously, you will need to open another MML session to perform any additional tasks. Refer to the “Starting an MML Session” section on page 3-2 for more information on starting additional MML sessions.

Understanding Alarms

The following subsections describe each of the message components for the typical alarm response shown below:

```
"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"
```

Component ID

The first element of the alarm message identifies the system component that generated the alarm, using the customer-defined description of the component given during system configuration. In our example, these are LPC-01, IOCM-01, MGC1alink2, and MGC1alink3.

All system components are described in the *Cisco Media Gateway Controller Software Release 7 Provisioning Guide*.

Time Stamp

The second element of the alarm message identifies the time of the alarm by year, month, day, hour, minute, hundredths, and thousandths of a second (milliseconds). The time displayed is the system time. In the example, these would be 2000-02-26 09:16:07.806, 2000-02-26 09:17:00.690, 2000-02-26 09:17:47.224, and 2000-02-26 09:17:47.225.

Alarm Category

The third element of the alarm message identifies the alarm category. It indicates the MML description of the alarm/event. In our example:

- ALM=\"SCMGC MTP3 COMM FAIL\" indicates an SCMGC-MTP3 communications failure.
- ALM=\"Config Fail\" indicates a configuration failure.
- ALM=\"SC FAIL\" indicates a signal channel failure.

Severity Level

The last element of the alarm message identifies the severity level of the alarm. The four levels are

- Critical (CR)—A serious problem exists in the network. Critical alarms cause a switchover, where the active Cisco MGC switches processing to the standby Cisco MGC. Because critical alarms affect service, they should be cleared immediately.

**Caution**

Critical alarms cause the system to automatically switchover. While a switchover is in progress, new calls are dropped and in-progress calls are sustained.

- **Major (MJ)**—A problem exists that disrupts service. Major alarms should be cleared immediately. These alarms differ from critical alarms in that they do not cause a switchover from the active Cisco MGC to the standby Cisco MGC.
- **Minor (MN)**—Minor alarms should be noted and cleared as soon as possible. You might also want to research how often this alarm is appearing, because it may be an indicator of a bigger problem.
- **Informational (IN)**—This severity level applies to messages that provide information about typical events and conditions. Informational messages do not require corrective action. Examples are timer expirations, values that have exceeded preset thresholds, and unexpected responses from endpoints to signaling messages sent by the Cisco MGC. Events with a severity level of informational are retrieved only by the SNMP Manager.

Verifying the Status of all Destinations

To verify the status of all of the destination point codes (DPCs) provisioned on your Cisco MGC, perform the following steps:

- Step 1** Log in to the active Cisco MGC, start an MML session, and enter the following command:

```
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"
"eisupftsvc:PKG=EISUP,ASSOC=SWITCHED,PST=IS,SST=UND"
"eisupsvc1:PKG=EISUP,ASSOC=SWITCHED,PST=IS,SST=UND"
```

**Note**

If the **rtrv-dest:all** MML command is entered 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 Cisco MGC has not received a service state message from the associated destination since the switchover occurred. No user action is required.

- Step 2** If the primary service state is *not* IS for any of the destinations, check your alarms retrieval MML session for signaling-related alarms. The method for setting up an alarms retrieval MML session is described in the “Monitoring the Alarms Status” section on page 3-6.

If a signaling-related alarm appears, you can determine the appropriate course of action by searching for the corrective actions for that alarm in the “Alarm Troubleshooting Procedures” section on page 8-8. If the alarm is not in that section, corrective action is not required. More information on the alarm can be found in the *Cisco Media Gateway Controller Software Release 7 Messages Reference Guide*.

You can also find additional information on the conditions that caused the alarms by viewing the system logs. The logs can be viewed using the log viewer, part of the Cisco MGC viewer toolkit. For information on using the log viewer, see the “Using the Log Viewer” section on page 3-114.

**Note**

You can also use the **rtrv-dest** MML command to retrieve information on individual destinations. For more information, refer to the *Cisco Media Gateway Controller Software Release 7 MML Command Reference Guide*.

Understanding the Destination State Information

The following sections describe the information returned by the system when you enter the **rtrv-dest** command, as in the example below:

```
"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"
```

Destination

The first field lists the MML name of the DPC. In the above example, this is dpc1, dpc2, and dpc3

Package

The PKG field lists the protocol package associated with the destination. In the example, the protocol is SS7-ANSI.

Association

The ASSOC field shows the type of association, either unknown, switched, or a specific channel for the destination. In the example, the association type is SWITCHED.

Primary Service State

The PST field shows the current primary service state of the destination. In the example, all of the destinations have a primary service state of IS. Table 3-2 lists the valid primary service state values:

Table 3-2 DPC Primary Service States

Link State ID	Link State	Description
AOOS	Automatically out-of-service	The system has taken the DPC out-of-service (OOS).
INB	Install busy	When a system is first configured, all signaling links default to this state and must be manually set in-service (IS) through the use of the set-sc-state MML command.
IS	In-service	The link to the DPC is IS and fully operational. This is its normal operating state.
MOOS	Manually out-of-service	The link to the DPC has been manually taken OOS.

Table 3-2 DPC Primary Service States (continued)

Link State ID	Link State	Description
OOS	Out-of-service	The link to the DPC is OOS from the remote end. The system is actively trying to restore the link.
TRNS	Transient	The state of the link to the DPC is currently being changed.
UNK	Unknown	The state of the link to the DPC is not known.

Secondary Service State

The SST field shows the current secondary service state of the specified destination. In the example, all of the DPCs have a secondary service state of UND. The valid states are listed below:

- CEA—Commanded into emergency alignment.
- CIS—Commanded in service.
- CONG—Congestion.
- COOS—Commanded out of service.
- CINH—Commanded to the inhibited state.
- CRTE—Created.
- CUINH—Commanded to the uninhibited state.
- DLT—Deleted.
- EIS—Engine in service.
- EOOS—Engine out of service.
- FLD—Failed.
- FOOS—Forced out of service.
- RST—Reset.
- RSTO—Restored.
- UND—Undefined.



Note

If the **rtrv-dest:all** MML command is entered 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 Cisco MGC has not received a service state message from the associated destination since the switchover occurred. No user action is required.

Verifying State of all SS7 Routes

To verify the status of all of the SS7 routes provisioned on your Cisco MGC, perform the following steps:

- Step 1** Log in to the active Cisco MGC, start an MML session, and enter the following command:

```
rtrv-rte:all
```

The system returns a message similar to the following:

```
MGC-01 - Media Gateway Controller 2001-05-22 11:35:46
M   RTRV
    "dpc1:linkset1,APC=244.001.040,PRIO=1,PST=IS,SST=NA"
    "dpc1:linkset2,APC=244.002.040,PRIO=1,PST=IS,SST=NA"
    "dpc2:linkset1,APC=244.001.041,PRIO=1,PST=IS,SST=NA"
    "dpc2:linkset2,APC=244.002.041,PRIO=1,PST=IS,SST=NA"
    "dpc4:linkset1,APC=244.001.044,PRIO=1,PST=IS,SST=NA"
    "dpc4:linkset2,APC=244.002.044,PRIO=1,PST=IS,SST=NA"
```

Step 2 If the primary service state is *not* IS for any of the routes, check your alarms retrieval MML session for signaling-related alarms. The method for setting up an alarms retrieval MML session is described in the “Monitoring the Alarms Status” section on page 3-6.

If a signaling-related alarm appears, you can determine the appropriate course of action by searching for the corrective actions for that alarm in the “Alarm Troubleshooting Procedures” section on page 8-8. If the alarm is not in that section, corrective action is not required. More information on the alarm can be found in the *Cisco Media Gateway Controller Software Release 7 Messages Reference Guide*.

You can also find additional information on the conditions that caused the alarms by viewing the system logs. The logs can be viewed using the log viewer, part of the Cisco MGC viewer toolkit. For information on using the log viewer, see the “Using the Log Viewer” section on page 3-114.

Understanding the SS7 Route State Information

The following sections describe the information returned by the system when you enter the **rtrv-rte** command, as shown in the example below:

```
"dpc1:linkset1,APC=244.001.040,PRIO=1,PST=IS,SST=NA"
"dpc1:linkset2,APC=244.002.040,PRIO=1,PST=IS,SST=NA"
"dpc2:linkset1,APC=244.001.041,PRIO=1,PST=IS,SST=NA"
"dpc2:linkset2,APC=244.002.041,PRIO=1,PST=IS,SST=NA"
```

Point Code

The first field lists the MML name for the target point code associated with the SS7 route. In the example, the point codes are dpc1 and dpc2.

Linkset

The second field lists the MML name for the linkset associated with the SS7 route. In the example, the linksets are linkset1 and linkset 2.

Adjacent Point Code

The APC field lists the point code for the adjacent point code (APC) associated with the SS7 route. In the example there are four point codes:

- 244.001.040
- 244.002.040
- 244.001.041
- 244.002.041

Priority

The PRIO field lists the priority provisioned for this SS7 route. In the example, all of the SS7 routes have a priority of 1.

Primary Service State

The PST field shows the current primary service state of the destination. In the example, all of the SS7 routes have a primary service state of IS. Table 3-2 lists the valid primary service state values:

Table 3-3 SS7 Route Primary Service States

Link State ID	Link State	Description
AOOS	Automatically out-of-service	The system has taken the SS7 route out-of-service (OOS).
INB	Install busy	When a system is first configured, all signaling links default to this state and must be manually set in-service (IS) through the use of the set-sc-state MML command.
IS	In-service	The SS7 route is IS and fully operational. This is its normal operating state.
MOOS	Manually out-of-service	The SS7 route has been manually taken OOS.
OOS	Out-of-service	The SS7 route is OOS from the remote end. The system is actively trying to restore the link.
TRNS	Transient	The state of the link to the DPC is currently being changed.
UNK	Unknown	The state of the link to the DPC is not known.

Secondary Service State

The SST field shows the current secondary service state of the specified destination. In the example, all of the SS7 routes have a primary service state of NA. The valid states are listed below:

- ACKD—SS7 Acknowledgement delay
- BSNR—SS7 backward sequence number received (BSNR)
- CIS—Commanded in service
- CONF—Configuration failure
- COOS—Commanded out of service
- ENGR—Call engine reset
- ISPEND—In service, pending
- LCNG—Congestion, local
- LINE—Line failure
- LINH—SS7 local inhibit
- LINK—Link failure
- LINS—Linkset failure
- NA—Cause not available
- OOSPEND—Out of service, pending

- PRHB—SS7 prohibited
- RBLK—SS7 remote blocked
- RCNG—Congestion, remote
- RINH—SS7 remote inhibit
- RSTR—SS7 restricted
- SERR—SS7 signal error
- STBY—Cause standby
- SUPPENT—Supporting entity
- TPATH—Traffic path
- UNK—Cause unknown

Verifying CIC States

We recommend verifying the status of your circuit identification codes (CICs) in groups, to ensure that you have current state information. Retrieving the status of all of your CICs at once can take a while to obtain, and then a long time to page through.

To verify the status of CICs provisioned on your Cisco MGC in groups, perform the following steps:

Step 1 Log in to the active Cisco MGC, start an MML session, and enter the following command:

```
rtrv-cic:dest_pc:cic=number[,rng=range]
```

Where:

- *dest_pc*—MML name of the DPC associated with the CICs to be displayed.
- *number*—A valid CIC number.
- *range*—Specifies a range of CICs to be retrieved. The status of all CICs between *number* and *number+range* are displayed.

For example, the MML command listed below retrieves bearer channel information for CICs 1-20 on destination point code dpc1:

```
rtrv-cic:dpc1:cic=1,rng=20
```

When the Cisco MGC software is used on a nailed network, the system returns a response similar to the following:

```
Media Gateway Controller - MGC-04 2000-04-05 08:05:54
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"
   "dpc1:CIC=10,PST=IS,CALL=IDLE,BLK=NONE"
   "dpc1:CIC=11,PST=IS,CALL=IDLE,BLK=NONE"
   "dpc1:CIC=12,PST=IS,CALL=IDLE,BLK=NONE"
   "dpc1:CIC=13,PST=IS,CALL=IDLE,BLK=NONE"
```

```
"dpc1:CIC=14,PST=IS,CALL=IDLE,BLK=NONE"
"dpc1:CIC=15,PST=IS,CALL=IDLE,BLK=NONE"
"dpc1:CIC=16,PST=IS,CALL=IDLE,BLK=NONE"
"dpc1:CIC=17,PST=IS,CALL=IDLE,BLK=NONE"
"dpc1:CIC=18,PST=IS,CALL=IDLE,BLK=NONE"
"dpc1:CIC=19,PST=IS,CALL=IDLE,BLK=NONE"
"dpc1:CIC=20,PST=IS,CALL=IDLE,BLK=NONE"
```

When the Cisco MGC software is used on a switched network, the system returns a response similar to the following:

```
Media Gateway Controller - MGC-04 2000-04-05 08:05:54
M RTRV
"dpc1:CIC=10,PST=IS,CALL=IDLE,GW_STAT=CNX_IS,BLK=NONE"
"dpc1:CIC=11,PST=IS,CALL=IDLE,GW_STAT=CNX_IS,BLK=NONE"
"dpc1:CIC=12,PST=IS,CALL=IDLE,GW_STAT=CNX_IS,BLK=NONE"
"dpc1:CIC=13,PST=IS,CALL=IDLE,GW_STAT=CNX_IS,BLK=NONE"
"dpc1:CIC=14,PST=IS,CALL=IDLE,GW_STAT=CNX_IS,BLK=NONE"
"dpc1:CIC=15,PST=IS,CALL=IDLE,GW_STAT=CNX_IS,BLK=NONE"
```

- Step 2** If the primary service state is *not* IS for any of the CICs, or a CIC is blocked, check your alarms retrieval MML session for bearer-related alarms. The method for setting up an alarms retrieval MML session is described in the “Monitoring the Alarms Status” section on page 3-6.

If a bearer channel-related alarm appears, you can determine the appropriate course of action by searching for the corrective actions for that alarm in the “Alarm Troubleshooting Procedures” section on page 8-8. If the alarm is not in that section, corrective action is not required. More information on the alarm can be found in the *Cisco Media Gateway Controller Software Release 7 Messages Reference Guide*.

Understanding CIC States

The elements of the output from the **rtrv-cic** MML command is described in the paragraphs that follow.

Circuit Identification

The output of this command identifies the MML name of the associated signaling channel and the number for each CIC.

Primary Service State

The PST field shows the current primary service state of the CIC. Table 3-4 lists the valid primary service state values:

Table 3-4 *CIC Primary Service States*

Link State ID	Link State	Description
IS	In-service	The traffic channel or CIC is IS and fully operational. This is its normal operating state.
OOS	Out-of-service	The traffic channel or CIC is OOS from the remote end. The system is actively trying to restore the link. Individual CICs can be OOS even if the destination is IS, due to signaling events such as Q.931 service messages.

Call State

The CALL field identifies the current call state of each CIC. After a call is initiated, a circuit does not return to the Idle (available) state until all related release signaling is satisfactorily completed (the correct release sequence). In and Out call states indicate that the CIC is not available for new calls. Table 3-5 describes the various call states.

Table 3-5 *CIC Call States*

State	Description
In	Incoming call is in progress. Bearer channel is not available for new call.
Out	Outgoing call is in progress. Bearer channel is not available for new call.
Idle	Circuit is available for use.

Media Gateway State

The GW_STAT field identifies the current state of the media gateway associated with each CIC. Table 3-6 describes the various media gateway states.

Table 3-6 *Media Gateway States*

State	Description
CARRIER_FAILURE	A carrier has failed. This is no longer a valid state as of Release 7.4(12).
INTERFACE_FAILURE	This state is valid in Release 7.4(12) and up. An individual CIC has failed. If this state is seen for all CICs associated with a T1 or E1, this indicates that the associated T1 or E1 has failed.
GW_HELD	The call has been held at the media gateway
CXN_IS	The connection is in service
CXN_OOS_ACTIVE	The connection is out of service on the active system
CXN_OOS_STANDBY	The connection is out of service on the standby system

Circuit Block Type

The BLK field identifies the type of circuit block that has been placed on the CIC. Blocked circuits are not available for calls. Table 3-7 describes the valid circuit block types.

Table 3-7 Circuit Block Types

Type	Description
GATEWAY	Locally blocked due to a media gateway event (for example, a media gateway interface fails causing an RSIP message to be sent, but the associated CICs remain in-service or when an RSIP message is not acted upon due to a mismatch between the MGCP host name in the RSIP string and the host name provisioned in the media gateway). If the associated switch is not responding to group unblock messages, the CICs stay in the GATEWAY circuit block state. Your CICs will be in this state when you bring up the Cisco MGC or media gateway. Once the associated switch acknowledges the unblock message, the CICs are taken out of this state. If the CICs stay in the GATEWAY circuit block state, troubleshoot the problem with the media gateway. As of Release 7.4(12), this value is used only for switched systems.
MATE_UNAVAIL	This state is valid in Release 7.4(12) and up, used only in nailed-up systems. Locally blocked due to a media gateway event (for example, a group service message received from the media gateway or the media gateway is out of service). If the associated switch is not responding to group unblock messages, the CICs stay in the MATE_UNAVAIL circuit block state. Your CICs will be in this state when you bring up the Cisco MGC or media gateway. Once the associated switch acknowledges the unblock message, the CICs are taken out of this state. If the CICs stay in the MATE_UNAVAIL circuit block state, troubleshoot the problem with the media gateway.
LOCAUTO	Hardware blocking type—the CIC is blocked by an external message generated by a network element outside the media gateway.
REMAUTO	Remotely automatically blocked.
LOCMAN	Blocked manually using an MML command, such as blk-cic . This is removable using the unblk-cic or reset-cic MML commands.
REMMAN	Remotely blocked manually.
LOCUNK	Locally blocked for unknown reasons. This indicates a potential software problem whereby a CIC has become blocked but the software did not track the cause of the blocking.
COT_FAIL	This state is valid in Release 7.4(12) and up. Blocked because a continuity test failed on the CIC.
INTERFACE_DISABLED	The interface is disabled because the system received a CGB message or a new service has been started which is still in the install busy (INB) state.
NONE	There is no block on the CIC. DS0 is available for use.

**Note**

Block types are additive: for example, LOCMAN (locally, manually blocked) and REMMAN (remotely, manually blocked) can both be active at the same time.

Verifying Available Disk Space

You should monitor the amount of disk space available on your Cisco MGC on a daily basis. The percentage of disk space capacity used should always be below 90 percent capacity. If your system's percentage of disk space capacity used 90 percent or higher, you must delete files from your disk drive. To verify your available disk space, perform the following steps:

- Step 1** Log in to the active Cisco MGC, and enter the following UNIX command to check the amount of available disk space on your system:

```
df -k
```

The system returns a response similar to the following:

Filesystem	kbytes	used	avail	capacity	Mounted on
/dev/dsk/c0t0d0s0	1018191	114909	842191	13%	/
/dev/dsk/c0t0d0s4	2056211	422774	1571751	22%	/usr

If the response to the command indicates a percentage of disk space capacity used 90 percent or higher, you must delete files from your disk drive, as described in the “Deleting Unnecessary Files to Increase Available Disk Space” section on page 8-112.

- Step 2** Repeat Step 1 and assess the command response. If the response indicates that the disk space usage is now below 90 percent of its capacity, then this procedure is complete. Otherwise, continue to delete files from your disk drive, as described in the “Deleting Unnecessary Files to Increase Available Disk Space” section on page 8-112, until the disk space usage drops below 90 percent of its capacity.

Verifying Available Virtual Memory

The operating system used on the Cisco MGC hosts, Solaris 2.6, is a virtual memory system. A virtual memory system adds to the available memory by writing the contents of an unused block of memory to the disk drive, enabling that block of memory to be used for another purpose. The space on the disk drive dedicated to this function is known as the swap space. Once the data in that block of memory is needed again, the system reads the stored block from the swap space back into memory.

In a typical Cisco MGC installation, the tmp directory (/tmp) is a temporary file system mount that coexists in the same physical disk partition as the swap space. The tmp directory is used to run a number of special files, such as FIFOs, that are required for the system to run properly. As the amount of space allocated to the tmp directory increases, the amount of space available for running Cisco MGC processes decreases, which can cause functional problems. You need to ensure that the amount of space consumed by the tmp directory is kept to a minimum.



Caution

Do not copy other files into the /tmp directory, such as patches or other software. Use of this directory for temporary storage or for downloading can cause functional problems with the Cisco MGC software.

To determine the amount of available virtual memory, you must compare the amount of virtual memory in use to the maximum amount of virtual memory for your system. To do this, perform the following steps:

**Note**

Be aware that the time of day at which you enter these commands affects the overall accuracy of the response. If you enter these commands during your busiest hours, the amount of available virtual memory could be quite small, but this may not indicate a need to contact the Cisco TAC.

If this is the case, consider also performing this procedure during a less active call processing time, to determine an average amount of available virtual memory.

- Step 1** The maximum amount of virtual memory is the sum of the physical memory and the size of the swap space. To determine the amount of physical memory on your system, log in to the active Cisco MGC and enter the following UNIX commands:

```
cd /usr/sbin
prtconf | grep Memory
```

The system returns a response similar to the following:

```
Memory size: 512 Megabytes
```

- Step 2** To determine the size of the swap space on the disk drive, enter the following UNIX command:

```
swap -s
```

The system returns a response similar to the following:

```
total: 57944k bytes allocated + 552816k reserved = 610760k used, 1359904k available
```

- Step 3** Add the amount of physical memory to the amount of swap space. This value is the maximum virtual memory for your system.

- Step 4** To determine the amount of available virtual memory, enter the following UNIX command:

```
vmstat
```

The system returns a response similar to the following:

```
procs      memory          page          disk          faults          cpu
 r  b  w   swap  free  re  mf  pi  po  fr  de  sr  s0  s1  s6  --   in   sy   cs  us  sy  id
 0   0   0   3176 22320   0   1   0   0   0   0   0   0   0   0   0   131  116  104   0   1  99
```

The amount of swap and free memory listed in the response (3176 and 22,320 in the above example) represents the total amount of available virtual memory. This amount should always be greater than 10 percent of the maximum virtual memory. If this is not the case, proceed to Step 5.

**Note**

You also can use this command to check the available virtual memory repeatedly. Enter it in the format **vmstat** *n*, where *n* is the number of seconds between checks. Refer to the man pages on the **vmstat** command for more information.

When the **vmstat** command is used to check the available virtual memory repeatedly, you should ignore the first line of output.

- Step 5** Contact the Cisco TAC for assistance. Refer to the “Obtaining Technical Assistance” section on page xviii for more information on contacting the Cisco TAC.

Verifying Available RAM

You should check the amount of available RAM on the Cisco MGC on a daily basis. To do this, perform the following steps:

- Step 1** Log in to the active Cisco MGC, and enter the following UNIX command to check the amount of available RAM on your system:

```
dmesg | grep mem
```

The system returns a response similar to the following:

```
mem = 2097152K (0x80000000)
avail mem = 2088370176
```

If the response indicates that you have plenty of memory available, the procedure is complete. If the response indicates that your system has a small amount of available memory, you may need to add additional memory to your Cisco MGC to handle your system’s call processing load.



Note Be aware that the time of day at which you enter this command will have an effect on the overall accuracy of the response. If you enter this command during your busiest hours, the amount of available memory could be quite small, but this may not indicate a need to add additional memory.

If this is the case, consider also performing this procedure during a less active call processing time, to determine an average amount of available memory.

- Step 2** Refer to your Sun Netra documentation for more information on how to add additional memory to a Cisco MGC host.

Verifying CPU Utilization Level

You should check the CPU utilization level on the Cisco MGC on a daily basis. To do this, log into the active Cisco MGC and enter the following UNIX command:

```
ps -ef -o user,pid,pcpu -o args
```

The system returns a response similar to the following:

```
va-herring% ps -ef -o user,pid,pcpu -o args
USER    PID  %CPU  COMMAND
root      0   0.0   sched
root      1   0.0   /etc/init -
root      2   0.0   pageout
root      3   0.1   fsflush
root    176   0.0   /usr/sbin/ntpd -s -w 172.24.239.41 171.69.10.2 171.69.4.143
172.24.24.16 198
root    152   0.0   /usr/lib/nfs/lockd
```

```

root 727 0.0 /usr/lib/saf/sac -t 300
root 175 0.0 /sbin/sh /etc/rc2.d/S74xntpd start
root 120 0.0 /usr/sbin/keyerv
root 118 0.0 /usr/sbin/rpcbind
root 190 0.0 /usr/sbin/nscd
root 145 0.0 /usr/sbin/inetd -s
daemon 150 0.0 /usr/lib/nfs/statd
root 167 0.0 /usr/lib/autofs/automountd
root 171 0.2 /usr/sbin/syslogd
root 324 0.0 /usr/sbin/rpc.bootparamd
root 184 0.0 /usr/sbin/cron
root 29986 0.0 in.rlogind
root 200 0.0 /usr/lib/lpsched
root 731 0.0 /usr/lib/saf/ttymon
root 9560 0.0 /opt/TimesTen32/32/bin/timestensubd -id 7
root 218 0.0 /usr/lib/power/powerd
root 228 0.0 /usr/lib/utmpd
mgcusr 9991 0.0 ../bin/cdrDmpr -X 30005
root 11085 0.0 /opt/CiscoMGC/bin/hostagt
mgcusr 29589 0.0 procM
root 10935 0.0 /opt/TimesTen32/32/bin/timestenrepld -id 8 -datastore
/opt/TimesTen32/datastore/
root 6396 0.0 ps -ef -o user,pid,pcpu -o args
root 10099 0.0 ../bin/foverd -X 30012
mgcusr 10097 0.0 ../bin/SS7 -X 30011
mgcusr 10095 0.1 ../bin/ISDNIP -X 3000c
mgcusr 10000 0.0 ../bin/pom -X 30008
root 294 0.0 /usr/sbin/vold
root 728 0.0 /usr/lib/saf/ttymon -g -h -p va-herring console login: -T sun -d
/dev/console
root 277 0.0 /usr/lib/sendmail -bd -q15m
root 11089 0.0 /opt/CiscoMGC/bin/fsagt
root 322 0.0 /usr/sbin/in.rarpd -a
root 9553 0.0 /opt/TimesTen32/32/bin/timestensubd -id 0
mgcusr 10096 0.0 ../bin/SS7 -X 30014
mgcusr 9990 0.0 ../bin/amDmpr -X 30004
root 11105 0.0 /opt/CiscoMGC/bin/snmpdm -tcplocal -d
mgcusr 10039 0.0 ../bin/replicator -X 3000d -C ../etc/XECfgParm.dat -t
root 10674 0.0 in.rlogind
root 10046 0.0 ../bin/sagt -X 3000a
root 27543 0.0 in.telnetd
root 9558 0.0 /opt/TimesTen32/32/bin/timestensubd -id 5
root 9557 0.0 /opt/TimesTen32/32/bin/timestensubd -id 4
mgcusr 10094 0.0 ../bin/TCAP -X 30010
root 9556 0.0 /opt/TimesTen32/32/bin/timestensubd -id 3
root 11106 0.0 /opt/CiscoMGC/bin/mib2agt -d
root 10042 0.0 ../bin/mmSagt -X 30009
mgcusr 10098 0.0 ../bin/SS7 -X 30013
root 11092 0.0 /opt/CiscoMGC/bin/critagt -d
haustin 10676 0.0 /usr/bin/tcsh
root 9559 0.0 /opt/TimesTen32/32/bin/timestensubd -id 6
root 9983 0.0 ../bin/almM -X 30002
root 9554 0.0 /opt/TimesTen32/32/bin/timestensubd -id 1
root 9555 0.0 /opt/TimesTen32/32/bin/timestensubd -id 2
mgcusr 10092 0.0 ../bin/mmdbd -X 30007
ipolat 28514 0.0 less platform_20010802040535.log
mgcusr 9981 0.1 ../bin/LogServerd -X 30015
root 9552 0.0 /opt/TimesTen32/32/bin/timestend
mgcusr 9997 0.0 ../bin/measMgr -X 30003
ricchen 29988 0.0 /usr/bin/tcsh
mgcusr 9994 0.0 ../bin/cfgM -X 30001
mgcusr 10034 0.0 ../bin/engine -X 3000e
root 10049 0.0 ../bin/provSagt -X 3000b
ricchen 24054 0.0 mml

```

```

root 1661 0.0 in.telnetd
mgcusr 1663 0.0 -csh
ipolat 27545 0.0 /usr/bin/tcsh
root 10093 0.0 ../bin/ioChanMgr -X 3000f

```

Check the percentage of CPU resources used for each process (found in the %CPU column). The response from the command represents a snapshot of CPU utilization. We recommend entering the UNIX command repeatedly to construct a more accurate picture of CPU utilization. If a process is using a large amount of CPU resources over an extended period of time, you should contact the Cisco TAC for assistance. Refer to the “Obtaining Technical Assistance” section on page xviii for more information on contacting the Cisco TAC.

Verifying the Number of Active Processes

You should check the number of active processes on the Cisco MGC on a daily basis. To do this, log into the active Cisco MGC and enter the following UNIX command:

```
ps -ef
```

The system returns a response similar to the following:

```

UID    PID  PPID  C   STIME TTY      TIME CMD
root    0    0    0 10:28:20 ?        0:00 sched
root    1    0    0 10:28:20 ?        0:27 /etc/init -
root    2    0    0 10:28:20 ?        0:00 pageout
root    3    0    0 10:28:20 ?        1:01 fsflush
root   174   173    0 10:29:03 ?        0:00 /usr/sbin/ntpddate -s -w 172.24.239.41
root   148    1    0 10:28:48 ?        0:00 /usr/lib/nfs/lockd
root   617    1    0 10:29:23 console 0:00 /usr/lib/saf/ttymon -g -h -p va-hoover console
login: -T sun -d /dev/console -
root   237    1    0 10:29:06 ?        0:00 /opt/TimesTen32/32/bin/timestend
root   116    1    0 10:28:36 ?        0:00 /usr/sbin/keyserv
root   114    1    0 10:28:36 ?        0:00 /usr/sbin/rpcbind
root   616    1    0 10:29:23 ?        0:00 /usr/lib/saf/sac -t 300
root   141    1    0 10:28:47 ?        0:00 /usr/sbin/inetd -s
daemon 146    1    0 10:28:48 ?        0:00 /usr/lib/nfs/statd
root   165    1    0 10:29:02 ?        0:11 /usr/lib/autofs/automountd
root   317    1    0 10:29:13 ?        0:00 /usr/sbin/rpc.bootparamd
root   169    1    0 10:29:02 ?        0:00 /usr/sbin/syslogd
root   173    1    0 10:29:02 ?        0:00 /sbin/sh /etc/rc2.d/S74xntpd start
root  2867   141    0 10:05:23 ?        0:00 in.telnetd
root   182    1    0 10:29:03 ?        0:00 /usr/sbin/cron
root   198    1    0 10:29:03 ?        0:00 /usr/lib/lpsched
root   227    1    0 10:29:05 ?        0:00 /usr/lib/utmpd
root   217    1    0 10:29:04 ?        0:00 /usr/lib/power/powerd
root   618    1    0 10:29:23 ?        0:00 /opt/CiscoMGC/bin/critagt -d
root   235    1    0 10:29:05 ?        0:00 /usr/lib/sendmail -bd -q15m
root   238   237    0 10:29:06 ?        0:00 /opt/TimesTen32/32/bin/timestensubd -id 0
root   239   237    0 10:29:06 ?        0:00 /opt/TimesTen32/32/bin/timestensubd -id 1
root   240   237    0 10:29:06 ?        0:00 /opt/TimesTen32/32/bin/timestensubd -id 2
root   241   237    0 10:29:06 ?        0:00 /opt/TimesTen32/32/bin/timestensubd -id 3
root   242   237    0 10:29:06 ?        0:00 /opt/TimesTen32/32/bin/timestensubd -id 4
root   243   237    0 10:29:06 ?        0:00 /opt/TimesTen32/32/bin/timestensubd -id 5
root   244   237    0 10:29:06 ?        0:00 /opt/TimesTen32/32/bin/timestensubd -id 6
root   245   237    0 10:29:06 ?        0:00 /opt/TimesTen32/32/bin/timestensubd -id 7
root   290    1    0 10:29:12 ?        0:00 /usr/sbin/vold
root   620   616    0 10:29:23 ?        0:00 /usr/lib/saf/ttymon
root   315    1    0 10:29:13 ?        0:01 /usr/sbin/in.rarpd -a
root   621   618    0 10:29:23 ?        0:05 /opt/CiscoMGC/bin/snmpdm -tcplocal -d
root   622   618    0 10:29:24 ?        0:00 /opt/CiscoMGC/bin/mib2agt -d
mgcusr  610    1    0 10:29:18 ?        0:02 procM

```

```

root      623      618    0 10:29:24 ?          0:00 /opt/CiscoMGC/bin/hostagt
root      624      618    0 10:29:24 ?          0:01 /opt/CiscoMGC/bin/fsagt
mgcusr    774      610    0 10:31:18 ?          0:17 ../bin/mmdbd -X 30007
mgcusr    626      610    0 10:29:24 ?          0:19 ../bin/LogServerd -X 30013
root      627      610    0 10:29:24 ?          0:05 ../bin/almM -X 30002
mgcusr    669      610    0 10:29:24 ?          0:08 ../bin/cdrDmpr -X 30005
mgcusr    637      610    0 10:29:24 ?          6:11 ../bin/amDmpr -X 30004
mgcusr    681      610    0 10:29:25 ?          0:11 ../bin/pom -X 30008
mgcusr    690      610    0 10:29:42 ?          0:02 ../bin/replicator -X 3000d -C ../
etc/XECfgParm.dat -t
mgcusr    670      610    0 10:29:24 ?          0:01 ../bin/cfgM -X 30001
mgcusr    673      610    0 10:29:25 ?          0:43 ../bin/measMgr -X 30003
mgcusr    689      610    0 10:29:42 ?          1:29 ../bin/engine -X 3000e
mgcusr    776      610    0 10:31:19 ?          0:01 ../bin/TCAP -X 30010
root      691      610    0 10:29:42 ?          0:01 ../bin/mmSAgt -X 30009
root      692      610    0 10:29:43 ?          0:04 ../bin/sagt -X 3000a
root      693      610    0 10:29:43 ?          0:01 ../bin/provSAgt -X 3000b
root      775      610    1 10:31:18 ?          37:37 ../bin/ioChanMgr -X 3000f
mgcusr    777      610    0 10:31:23 ?          0:12 ../bin/MGCP -X 30016
mgcusr    778      610    0 10:31:23 ?          0:27 ../bin/ISDNL3 -X 3000c
mgcusr    779      610    0 10:31:23 ?          0:26 ../bin/ISDNL3 -X 30011
mgcusr    780      610    0 10:31:23 ?          0:30 ../bin/ISDNL3 -X 30014
mgcusr    781      610    0 10:31:23 ?          0:01 ../bin/ISDNL3 -X 30015
mgcusr    782      610    0 10:31:23 ?          0:42 ../bin/SS7 -X 30017
root      783      610    0 10:31:23 ?          0:05 ../bin/foverd -X 30012
mgcusr2 5458      5456    0 11:07:28 pts/0      0:00 -tcsh
root      5456     141    0 11:07:28 ?          0:00 in.rlogind
root      367       1    0 14:21:02 ?          0:00 /usr/sbin/nscd
mgcusr    2869     2867    0 10:05:23 pts/1      0:00 -csh
root      3101     2869    0 10:06:49 pts/1      0:00 ps -ef

```

The response should indicate that there are between 60 and 100 processes active. If the response indicates that there are more than 100 active processes, you should contact the Cisco TAC for assistance. Refer to the “Obtaining Technical Assistance” section on page xviii for more information on contacting the Cisco TAC.

Verifying the Number of Users

You should check the number of users on the Cisco MGC on a daily basis. To do this, log into the active Cisco MGC and enter the following UNIX command:

```
who
```

The system returns a response similar to the following:

```

mgcusr pts/0          May 29 11:07      (mgcusr-u5.somecompany.com)
mgcusr2 pts/1          May 30 10:05      (mgcusr2-u6.somecompany.com)

```

Only known login IDs should be listed in the response. If the response indicates that there are unknown login IDs, or login sessions that have lasted a very long time, you should contact the Cisco TAC for assistance. Refer to the “Obtaining Technical Assistance” section on page xviii for more information on contacting the Cisco TAC.

Verifying Available Memory on the Cisco SLTs

You should check the amount of available memory on your Cisco Signaling Link Terminals (SLTs) on a daily basis. To do this, perform the following steps:

Step 1 Log in to a Cisco SLT, and enter the following IOS command to check the amount of available memory:

```
show mem
```

The system returns a response similar to the following:

	Head	Total (b)	Used (b)	Free (b)	Lowest (b)	Largest (b)
Processor	80CF71E0	16813600	7885028	8928572	8900652	8891892
I/O	1D00000	19922944	6975904	12947040	12938256	12937500

Ensure that the memory used is less than 90 percent of the total available memory. If this is the case, the procedure is complete. If the response indicates that the Cisco SLT has a small amount of available memory, you may need to add additional memory to the Cisco SLT to handle your system's call processing load.



Note Be aware that the time of day at which you enter this command will have an effect on the overall accuracy of the response. If you enter this command during your busiest hours, the amount of available memory could be quite small, but this may not indicate a need to add additional memory.

If this is the case, consider also performing this procedure during a less active call processing time, to determine an average amount of available memory.

Step 2 Refer to the "Upgrading DRAM" section on page 6-16 for more information on how to add additional memory to a Cisco SLT.

Periodic Maintenance Procedures

This section contains procedures that are either performed on automatically, on a scheduled basis, by the system or should be performed by you on a regular basis to keep the Cisco MGC node operating smoothly. You should schedule the procedures that are performed manually as you see fit. These maintenance procedures include

- Automatic Disk Space Monitoring, page 3-24
- Automatic System Log Rotation, page 3-27
- Rotating System Logs Manually, page 3-27
- Creating a Disaster Recovery Plan, page 3-27
- Backing Up System Software, page 3-28



Note

This section does not include information on maintaining the Sun host server hardware. You should routinely perform general maintenance tasks and diagnostic checks on the host hardware. See the documentation provided by Sun Microsystems, the hardware manufacturer, for detailed information on these types of procedures.

Automatic Disk Space Monitoring

The Cisco MGC software includes a script called disk monitor (`diskmonitor.sh`) that periodically checks the amount of disk space used within the configurable set of disk partitions. Disk monitor ensures that there is sufficient disk space available in each disk partition for the system to continue to operate at peak performance. To do this, disk monitor deletes (trims) the older log files in the `/opt/CiscoMGC/var/log` and `/opt/CiscoMGC/var/spool` directories until the disk space usage is within the specified threshold (set using the `XECfgParm.dat` parameter, `diskmonitor.Threshold`).

The disk monitor can also track the number of configurations stored in the configuration library (which is found in the `/opt/CiscoMGC/etc/CONFIB_LIB` directory) and trim the older configurations when the number of configurations exceeds the maximum value you have set in the associated `XECfgpParm.dat` disk monitor parameter. The process manager runs the disk monitor script once every minute.

The process of administering the configuration library is handled automatically by the Cisco MGC software. The user sets the disk monitor parameter to establish the maximum number of configurations allowed in the configuration library, and the system will trim the older configurations as necessary.

Disk monitor is controlled using the following parameters in the `XECfgParms.dat` file:

- `diskmonitor.Limit`—Specifies the number of days to preserve data before trimming is initiated. The default value is 7.
- `diskmonitor.OptFileSys`—List of optional file systems to monitor. These files are not trimmed by disk monitor.
- `diskmonitor.Threshold`—Specifies the percentage of disk usage at which alarming and disk trimming is initiated. The default value is 80.
- `diskmonitor.CdrRmFinished`—Specifies how many days to keep finished (polled) call detail record (CDR) files. The default value is 0, which means that finished CDRs are immediately sent to the spool directory.
- `diskmonitor.SoftLimit`—Specifies the action to be taken once the number of days threshold set in the `diskmonitor.Limit` parameter is reached. If this parameter is set to *true*, disk monitor decrements the value in the `diskmonitor.Limit` parameter one day at a time (that is, from 7 down to 6, and then down to 5, and so on) until the utilization level drops below the threshold. If this parameter is set to *false*, disk monitor closes and the system generates a DISK alarm. The files can then be deleted manually. The default value is *false*.
- `diskmonitor.CfgRmDirs`—This parameter is added as of release 7.4(11). This parameter specifies the maximum number of configurations that can be stored in the configuration library. The valid values are the range of integers from 3 through 64. The default value is 64. Entering a value outside of the range of valid values disables monitoring of the number of entries stored in the configuration library. If you want to change the value of this parameter, you may need to add it manually to the `XECfgParm.dat` file.

As of Release 7.4(11), disk monitor performs the following steps in its inspection of disk utilization levels:

1. Verify that the standard and optional partitions, as defined in `diskmonitor.OptFileSys`, are not over the thresholds for disk utilization or the configuration library, as defined in `diskmonitor.Threshold` and `diskmonitor.CfgRmDirs`, respectively.
 - a. If neither threshold is exceeded, disk monitor exits.
 - b. If the disk utilization threshold is exceeded, disk monitor attempts to trim the files based on the number of days, as defined in `diskmonitor.Limit`.

- c. If the configuration library threshold is exceeded, disk monitor trims the number of configuration files to match the setting in the `diskmonitor.CfgRmDirs` parameter, starting with the oldest.
2. Once files are trimmed, disk monitor verifies again that the standard and optional partitions are not over the thresholds for disk utilization and the configuration library.
 - a. If neither threshold is exceeded, disk monitor exits.
 - b. If the disk utilization threshold is exceeded, and `diskmonitor.SoftLimit` is set to false, the disk monitor is exited and a DISK alarm is raised.
 - c. If the disk utilization threshold is exceeded, and `diskmonitor.SoftLimit` is set to true, disk monitor begins decreasing the number of days that logs can be stored (the value defined in `diskmonitor.Limit`), stopping as soon as the disk is under the disk utilization threshold.
 - d. If the configuration library threshold is exceeded, disk monitor trims the number of configuration files to match the setting in the `diskmonitor.CfgRmDirs` parameter, starting with the oldest.

If any disk partition exceeds the configurable usage threshold, the Cisco MGC generates a DISK alarm (a major alarm), a warning of a disk partition overrun, and a warning of insufficient disk space. Refer to the “DISK” section on page 8-26 for information about the corrective actions required to resolve a DISK alarm.

Some other files, such as call trace files, take up large amounts of disk space and are not trimmed by disk monitor. You may have to periodically delete call trace files. Call trace files are created when you perform call traces as part of troubleshooting a problem. These files can be rather large, and leaving them on your disk could cause problems. For more information about deleting call trace files, refer to the “Deleting Unnecessary Files to Increase Available Disk Space” section on page 8-112.

**Caution**

If you are using software prior to Release 7.4(11), we recommend that you limit the number of configuration versions stored in the configuration library to 64. If you are storing a more than 64 system configurations, the state transition can fail during a switchover operation or use of the **prov-sync** MML command, and the standby Cisco MGC goes to an OOS state. For more information about administering the configuration library, refer to the “Using the Config-Lib Viewer” section on page 3-113.

Configuring Disk Monitor

Configuration of the disk monitor can only be done while the Cisco MGC software is turned off. For this reason, disk monitor is typically configured only during the initial installation. For more information on configuring the disk monitor during initial installation, refer to the `XECfgParms.dat` section of the *Cisco Media Gateway Controller Software Release 7 Installation and Configuration Guide*.

You can perform the configuration after initial installation. To do this, perform the following steps:


Caution

Performing the following procedure requires that the Cisco MGC software be turned off. Do not attempt the following procedure without the guidance of the Cisco TAC. Refer to the “Obtaining Technical Assistance” section on page xviii for more information about contacting the Cisco TAC.

If your system uses a single Cisco MGC in a simplex configuration, performing this procedure causes you to drop all calls.

Step 1 Determine whether any alarms are pending on the active Cisco MGC, as described in the “Retrieving All Active Alarms” section on page 8-3.

If any alarms are pending, you can determine the appropriate courses of action by searching for the corrective actions for those alarms in the “Alarm Troubleshooting Procedures” section on page 8-8. If the alarms are not in that section, corrective action is not required. More information on those alarms can be found in the *Cisco Media Gateway Controller Software Release 7 Messages Reference Guide*.

Step 2 Repeat Step 1 for the standby Cisco MGC.

Step 3 Modify the disk monitor parameters in the XECfgParm.dat files, which are listed below, on each host, using the procedure described in the “Rebooting Software to Modify Configuration Parameters” section on page 8-125.

- `diskmonitor.Limit` parameter—Sets the number of days to preserve logged data before trimming is initiated. The default value is 7.
- `diskmonitor.OptFileSys`—Sets the optional file systems that are checked by the disk monitor script.


Note

Files in optional directories are not trimmed by disk monitor.

- `diskmonitor.Threshold`—Sets the percentage of disk usage at which alarming and disk trimming is initiated. The default value is 80.
- `diskmonitor.CdrRmFinished`—Sets the number of days that finished CDR files are kept in the log directory. The default value is 0, which means that finished CDR files are immediately sent to the spool directory.
- `diskmonitor.SoftLimit`—Determines what action is taken once the number of days threshold set in the `diskmonitor.Limit` parameter is reached. If this parameter is set to *true*, disk monitor decrements the value in the `diskmonitor.Limit` parameter one day at a time (that is, from 7 down to 6 then down to 5 and so on), until the utilization level drops below the threshold. If this parameter is set to *false*, disk monitor exits and the system generates a DISK alarm. The default value is *false*.
- `diskmonitor.CfgRmDirs`—As of Release 7.4(11), you can set the maximum number of configurations that can be stored in the configuration library. The valid values are the range of integers from 3 through 64. The default value is 64. This parameter is not present in the XECfgParm.dat file initially. If you want to modify the value, you must enter the parameter manually into the file.


Caution

The Cisco MGC software is case-sensitive. Ensure that you enter the parameter name correctly, or the maximum number of configurations will not be modified.

**Note**

If you want to ensure the proper functioning of the **prov-sync** MML command, set the `diskmonitor.CfgRmDirs` parameter to a value between 50 and 60. Entering a value outside of the range of valid values (3 through 64) disables monitoring of the number of entries stored in the configuration library.

Automatic System Log Rotation

As the system operates, the Cisco MGC software creates the system logs that are stored in a file stored in the `/opt/CiscoMGC/var/log` directory. The name of the system log file is set by the `XECfgParm.dat` file parameter, `logFileNamePrefix` (the default value is *platform*). The Cisco MGC software stops writing to the current system log file, archives the contents of that file, and commences writing to a new system log file. This process is referred to as log rotation.

Log rotation occurs as a result of one of the following conditions:

- Cisco MGC software startup (the log rotation script is run)
- Log rotation script (`log_rotate.sh`) is run manually
- The size of the active system log file has exceeded the value set in the `XECfgParm.dat` parameter, `fileRotateSize`.
- The time elapsed since the last log rotation has exceeded the value set in the `XECfgParm.dat` parameter, `fileRotateInterval`.

When the system rotates the system log file, the current system log file is archived and a new system log file is opened. The archived log file is stored in the `$BASEDIR/var/spool` directory. Once the Cisco MGC software is up and running, the log server takes over the actual file rotation responsibility of renaming the active file to a historical file with a new file name with the following format:

`logFileNamePrefix_yyyymmddhhmmss.log`, where the time stamp indicates the date/time from the system at the time of rotation.

Rotating System Logs Manually

You can also run the log rotation script manually to force the current system log file to be archived. To do this, log into the active Cisco MGC as root, and enter the following UNIX command:

```
/opt/CiscoMGC/bin/log_rotate.sh
```

The system creates a new current system log file and archived log file, as described in the “Automatic System Log Rotation” section on page 3-27.

Creating a Disaster Recovery Plan

You should formulate a disaster recovery plan for your Cisco MGC node to ensure that your system can be restored to service quickly after it has been taken out-of-service by a natural or man-made disaster. A key element in your disaster recovery plan should be ensuring that regular backups of your system’s software are performed. Refer to the “Backing Up System Software” section on page 3-28 for more

information about backup operations. We also recommend that the backup data for your system be stored in a secure location, in a site separate from the equipment, to ensure that they are not affected by the same disaster.

For information on recovering from a natural or man-made disaster, refer to the “Recovering from Cisco MGC Host(s) Failure” section on page 8-115.

Backing Up System Software

You should perform regularly scheduled system software backups on both the active and standby Cisco MGCs to protect critical system data such as configuration files, which are irreplaceable if lost. If a catastrophic failure occurs, it is much easier to restore system information from backup data than to recreate it. Furthermore, such a failure could cause critical configuration information to be lost if it has not been backed up. We recommend that you create a backup schedule, ensuring that small or incremental backups are performed daily, and a large or full backup once a week.

**Note**

We recommend that you back up your system software during periods of low call volume to minimize the effect of the backup on your call processing.

There are two backup methods available for the Cisco MGC software, one for software releases up to 7.4(10), and another for software releases from 7.4(11) and up. These backup methods are described in the following sections:

- Backup Procedures for Cisco MGC Software up to Release 7.4(10), page 3-28
- Backup Procedures for Cisco MGC Software from Release 7.4(11) and up, page 3-33

Backup Procedures for Cisco MGC Software up to Release 7.4(10)

This backup method uses a script to backup the configuration data for the Cisco MGC software on to either a local tape drive or on to a remote machine. This script also allows you to perform full or partial backups. Backup of the Main Memory Database (MMDB) is performed by a separate script. These scripts do not enable you to schedule automatic backup times. You must perform these backups manually.

**Note**

If your Cisco MGC is a continuous service system, ensure that you perform backup procedures on both Cisco MGC hosts.

The following sections provide the backup procedures:

- Storing a Full Backup Operation on a Local Tape, page 3-29
- Storing a Partial Backup Operation on a Local Tape, page 3-29
- Storing a Full Backup Operation on a Remote Machine, page 3-30
- Storing a Partial Backup Operation on a Remote Machine, page 3-32
- Regular Operations, page 3-39

**Note**

The procedures for restoring system data can be found in the “Restoring Procedures for Cisco MGC Software up to Release 7.4(10)” section on page 8-118.

Storing a Full Backup Operation on a Local Tape

Use this procedure to store the results of a full backup operation (everything under the base directory) to a tape inserted in the local tape drive. To do this, complete the following steps:

-
- Step 1** Log in to the active Cisco MGC as root and change directories to a local subdirectory under the base directory.
- For example, enter the following command to change to the /opt/CiscoMGC/local directory:
- ```
cd /opt/CiscoMGC/local
```
- 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 “Regular Operations” section on page 3-39.
- 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** 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 5** When the backup operation has finished, remove the tape, engage the write-protect tab, and label the tape "Full MGC Backup." Specify the machine name and the time and date.
-

Storing a Partial Backup Operation on a Local Tape

Use this procedure to store a partial backup operation (the contents of the etc, local, var, and dialPlan subdirectories under the MGC base directory) to a tape inserted in a local tape drive. To do this, complete the following steps:

-
- Step 1** Log in to the active Cisco MGC as root and change directories to a local subdirectory under the base directory.

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

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

- 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 “Regular Operations” section on page 3-39.

- 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 **P** and press **Enter** to start the partial backup. The system returns a response 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 blocksL
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 5** When the backup operation has finished, remove the tape, engage the write-protect tab, and label the tape "Partial MGC Backup." Specify the machine name and the time and date.

Storing a Full Backup Operation on a Remote Machine

Use this procedure to store a full backup operation (everything under the MGC 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 can be written to by the machine being backed up. The NFS setup of the remote machine is beyond the scope of this procedure.



Note

The remote NFS server you select to store your back up data should be a system in your network that is not used as a Cisco MGC. Storing back up data on a Cisco MGC can negatively affect the performance of the system.

To back up the entire Cisco MGC software directory to a remote machine, complete the following steps:

-
- Step 1** Log in to the active Cisco MGC as root and change directories to a local subdirectory under the base directory.
- For example, enter the following command to change to the /opt/CiscoMGC/local directory:
- ```
cd /opt/CiscoMGC/local
```
- 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 “Regular Operations” section on page 3-39.
- 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 **F** and press **Enter** to start the full backup. The system returns a response similar to the following:
- ```
a ./ 0 tape blocks
a ./var/ 0 tape blocks
a ./var/log/ 0 tape blocks
.
.
.

backup to va-panthers:/backup/va-blade20000317105337.tar complete
#
```
- The filename on the remote NFS server is the host name of the machine with the date in YYYYMMDDHHMMSS format and “.tar” appended.
-

Storing a Partial Backup Operation on a Remote Machine

Use this procedure to store a partial backup operation (the contents of the etc, local, var, and dialPlan subdirectories under the MGC base directory) to an NFS mountable directory on a remote machine. The remote machine must be set up with an NFS mountable directory that can be written to by the machine being backed up. The NFS setup of the remote machine is beyond the scope of this procedure.



Note

The remote NFS server you select to store your back up data should be a system in your network that is not used as a Cisco MGC. Storing back up data on a Cisco MGC can negatively affect the performance of the system.

To back up a portion of the Cisco MGC software directory to a remote machine, complete the following steps:

-
- Step 1** Log in to the active Cisco MGC as root and change directories to a local subdirectory under the base directory.
- For example, enter the following command to change to the /opt/CiscoMGC/local directory:
- ```
cd /opt/CiscoMGC/local
```
- 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 “Regular Operations” section on page 3-39.
- 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.

### Performing a Backup Operation on the Main Memory Database

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



#### Note

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

- Step 1** Log in to the active Cisco MGC and 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

```

Backup Procedures for Cisco MGC Software from Release 7.4(11) and up

This backup method uses a script to backup the configuration data for the Cisco MGC software, select UNIX administrative files, and the Main Memory Database (MMDB). This script only performs full backups. This script enables you to perform manual backups, schedule and administer automatic backups, and view a history of the last 30 backup operations performed.

**Note**

This functionality is part of a patch to Release 7.4(11). If you want to use this functionality, you must be upgraded to the proper patch level. For more information on verifying the patch level of your system, refer to the “Verifying the Patch Level of the Cisco MGC” section on page 3-85.

**Note**

If your Cisco MGC is a continuous service system, ensure that you perform backup procedures on both Cisco MGC hosts.

**Note**

The procedures for restoring system data can be found in the “Restoring Procedures for Cisco MGC Software Release 7.4(11) and up” section on page 8-121.

The following sections provide the backup procedures:

- Performing a Manual Backup Operation, page 3-34
- Scheduling an Automatic Backup Operation, page 3-35
- Listing Scheduled Automatic Backup Operations, page 3-37
- Removing an Automatic Backup Operation from the Schedule, page 3-38
- Listing the Backup Operation History, page 3-39

Performing a Manual Backup Operation

To perform a manual backup operation, enter the following UNIX command on the Cisco MGC:

```
mgcbbackup -d path [-r retries -t retry_time]
```

Where:

- *path*—The full path of the directory in which to store the backup file, for example a directory on a remote server that you have mounted on your system, or the local tape drive.

**Note**

We recommend that you do not store backup files on your local Cisco MGC host, as storage of backup files on the local host reduces the amount of disk space available to process call data, and does not ensure that the data is safe in the event of a natural disaster.

**Note**

If the path you enter is for a tape device, be aware that a new tape must be entered into the device for each backup. The backup data on a used tape will be overwritten by this operation.

- *retries*—The number of times to check for an active provisioning session on the Cisco MGC, before aborting the backup operation. The default value is 0, and the maximum value is 100.

**Note**

A backup operation cannot start while there is an active provisioning session on the Cisco MGC.

- *retry_time*—The number of seconds to wait between checks for an active provisioning session on the Cisco MGC. The default value is 30 seconds, and the maximum value is 3600 seconds.

For example, to perform a manual backup operation where the backup file is saved to a directory path called /dev/rmt/h0, with a maximum of three attempts, each 60 seconds apart, you would enter the following UNIX command:

```
mgcbbackup -d /dev/rmt/h0 -r 3 -t 60
```

The backup file is stored in the specified directory path in the following format:

```
mgc_hostname_yyyymmdd_hhmmss_backup
```

Where:

- *hostname*—The name of the Cisco MGC host, such as MGC-01.
- *yyymmdd*—The date the backup file is created, in a year-month-day format, such as 20011130.
- *hhmmss*—The time the backup file is created, in an hour-minute-second format, such as 115923.

Scheduling an Automatic Backup Operation

To schedule an automatic backup operation, perform the following steps:



Note

You can schedule an automatic backup operation when you are logged in to your system as either *root* or *mgcusr*. Any backups scheduled while you are logged in as *root* cannot be seen while you are logged in as *mgcusr*. For that reason, we recommend that you always log in as *mgcusr* when scheduling an automatic backup operation.

Step 1 Enter the following UNIX command on the Cisco MGC:

```
mgcbbackup -s
```

The system returns a response similar to the following:

```
Backup Schedule Menu
-----
```

1. Add a scheduled backup
2. Delete a scheduled backup
3. List scheduled backups
4. Exit

Selection:

Step 2 Enter **1** to add an automatic backup operation to the schedule.

The system returns a response similar to the following:

```
Add a Scheduled Backup
-----
```

Enter the name of the backup:

Step 3 Enter the name of your backup.



Note

The name of the backup can only be between 1 and 10 alphanumeric characters in length.

After you enter the name of your automatic backup, the system returns a response similar to the following:

Enter the directory to place the backup file:

Step 4 Enter the directory path where you want the backup file stored.



Note We recommend that you do not store backup files on your local Cisco MGC host, as storage of backup files on the local host reduces the amount of available disk space to process call data, and does not ensure that the data is safe in the event of a natural disaster.



Note If the path you enter is for a tape device, be aware that a new tape must be entered into the device for each backup. The backup data on a used tape will be overwritten by this operation.

After you enter your directory path, the system returns a response similar to the following:

Enter the number of retries (default=0):

Step 5 Enter the number of times to check for an active provisioning session on the Cisco MGC before aborting the backup operation.



Note A backup operation cannot start while a provisioning session is active on the Cisco MGC.



Note The maximum number of retries is 100.

After you enter the number of retries, the system returns a response similar to the following:

Enter the time between retries (default=30 seconds):

Step 6 Enter the number of seconds to wait between checks for an active provisioning session on the Cisco MGC.



Note The maximum number of seconds between checks is 3600.

After you enter the time between attempts, the system returns a response similar to the following:

Enter the day of the week (default=everyday):

Step 7 Enter the day(s) of the week that you would like the backup operation performed. The following values are valid:

- SUNDAY
- MONDAY
- TUESDAY
- WEDNESDAY
- THURSDAY
- FRIDAY
- SATURDAY

- WEEKDAYS
- WEEKENDS
- EVERYDAY

After you enter your day(s) of the week setting, the system returns a response similar to the following:

Enter the time (HH:MM):

Step 8 Enter the time to start your automatic backup operation, in hour:minute format.



Note

The range for hour is 00-23, and the range for minute is 00-59.



Note

We recommend that you schedule your automatic backup operation for a time when your system is likely to have a minimum amount of call volume to minimize the effect of the backup on your call processing.

After you enter your time setting, the system returns a response similar to the following:

Press enter to continue:

Step 9 Press enter to return to the backup schedule menu. You can either exit the utility or perform another backup scheduling activity.

When the automatic backup operation is performed, the backup file is stored in the specified directory path in the following format:

```
mgc_hostname_yyyymmdd_hhmmss_backup.tar
```

Where:

- *hostname*—The name of the Cisco MGC host, such as MGC-01.
- *yyymmdd*—The date the backup file is created, in a year-month-day format, such as 20011130.
- *hhmmss*—The time the backup file is created, in a hour-minute-second format, such as 115923.

Listing Scheduled Automatic Backup Operations

To list the scheduled automatic backup operations, perform the following steps:

Step 1 Enter the following UNIX command on the Cisco MGC:

```
mgcbakup -s
```

The system returns a response similar to the following:

```
Backup Schedule Menu
```

```
-----
```

1. Add a scheduled backup
2. Delete a scheduled backup
3. List scheduled backups
4. Exit

Selection:

Step 2 Enter 3 to list the scheduled automatic backup operations.

The system returns a response similar to the following:

```
Scheduled Backups
-----
```

| Name | Retries | Timeout | Day | Time | Directory |
|----------|---------|---------|----------|-------|------------|
| Back1 | 5 | 60 | everyday | 12:00 | /var/cisco |
| Mybackup | 0 | 30 | weekdays | 04:00 | /var/cisco |

Press enter to continue:

- Step 3** Press enter to return to the backup schedule menu. You can either exit the utility or perform another backup scheduling activity.
-

Removing an Automatic Backup Operation from the Schedule

To remove an automatic backup operation from the schedule, perform the following steps:

- Step 1** Enter the following UNIX command on the Cisco MGC:

```
mgcbbackup -s
```

The system returns a response similar to the following:

```
Backup Schedule Menu
-----
```

1. Add a scheduled backup
2. Delete a scheduled backup
3. List scheduled backups
4. Exit

Selection:

- Step 2** Enter **2** to remove an automatic backup operation from the schedule.

The system returns a response similar to the following:

```
Delete a Scheduled Backup
-----
```

Enter the name of the backup:

- Step 3** Enter the name of the automatic backup operation you want to remove from the schedule.

The system returns a response similar to the following:

Press enter to continue:

- Step 4** Press enter to return to the backup schedule menu. You can either exit the utility or perform another backup scheduling activity.
-

Listing the Backup Operation History

To see a history of the last 30 backup operations, perform the following steps:

Step 1 Enter the following UNIX command on the Cisco MGC:

```
mgcbbackup -l
```

The system returns a response similar to the following:

```
Status File
Success /var/Cisco/mgc_venus_20011010_153003_backup
Success /var/Cisco/mgc_venus_20011011_153003_backup
Success /var/Cisco/mgc_venus_20011012_153003_backup
```

Press enter to continue:



Note If a backup operation fails, the reason for the failure is listed below the file name.

Step 2 Press enter to return to the backup schedule menu. You can either exit the utility or perform another backup scheduling activity.

Regular Operations

This section contains procedures that you can perform on your Cisco MGC as needed. The regular operations are described in the following sections:

- Managing MML Sessions, page 3-39
- Managing Signaling Channels, page 3-47
- Managing Bearer Channels, page 3-55
- Provisioning your Cisco MGC, page 3-63
- Managing your Cisco MGC Platform, page 3-80
- Managing System Measurements, page 3-90
- Using the Cisco MGC Viewer Toolkit, page 3-102

Managing MML Sessions

The operations you can use to manage an MML session are described in the following sections:

- Displaying Previously Entered MML Commands, page 3-40
- Displaying Information About MML Commands, page 3-41
- Reentering Previously Entered MML Commands, page 3-46
- Retrieving Active MML Sessions, page 3-47
- Ending an MML Session, page 3-47

Displaying Previously Entered MML Commands

You can use the **h** MML command to redisplay an MML command or a series of MML commands, depending on the number or range that you enter. If you do not enter a number or range, the last MML command entered is displayed.

To redisplay the last MML command entered, log in to the active Cisco MGC, start an MML session, and enter the following command:

h

The system returns a response similar to the following:

```
Media Gateway Controller - MGC-01 2000-01-12 15:19:51
M  RTRV
    "RTRV-TC:ALL"
    /* command 1 */
```

To redisplay a particular MML command that you entered, log in to the active Cisco MGC, start an MML session, and enter the following command:

h: :number

Where *number* is the number of the MML command you want to display. The last MML command you entered is equal to 1, the command you entered before that would be equal to 2, and so on.

For example, to redisplay the tenth most recently entered MML command, you would enter the following command:

h: :10

The system returns a response similar to the following:

```
Media Gateway Controller - MGC-01 2000-01-12 15:19:51
M  RTRV
    "RTRV-SC:ALL"
    /* command 10 */
```

To redisplay a range of MML command that you entered, log in to the active Cisco MGC, start an MML session, and enter the following command:

h: :start_num,end_num

Where:

- *start_num*—The number of the first MML command you want to display. The last MML command you entered is equal to 1, the command you entered before that would be equal to 2, and so on.
- *end_num*—The number of the last MML command you want to display.

For example, to redisplay all of the commands from the second to the fifth most recently entered MML commands, you would enter the following command:

h: :2,5

The system returns a response similar to the following:

```
Media Gateway Controller - MGC-01 2000-01-12 15:19:51
M  RTRV
    "RTRV-SC:ALL"
    /* command 5 */
    "RTRV-SOFTW:ALL"
    /* command 4 */
    "RTRV-TC:ALL"
    /* command 3 */
```



```
"STP-AUD"
/* command 2 */
```

Displaying Information About MML Commands

You can use the **help** MML command to display information on all MML commands or detailed information on individual commands. To display information on a specific MML command, log in to the active Cisco MGC, start an MML session, and enter the following command:

```
help:command_name
```

Where *command_name* is the name of the MML command for which you want information.

For example, if you wanted information on the **set-log** MML command, you would enter the following command:

```
help:set-log
```

The system would return a response similar to the following:

```
Media Gateway Controller - MGC-03 2000-03-20 10:04:28
```

```
M RTRV
```

```
SET-LOG -- Set Logging Levels
-----
```

```
Purpose:      This MML command is used to set the logging level of a
              process or all processes.
```

```
Format:      set-log:<proc>:<log level>
              set-log:all:<log level>
```

```
Input
Description:  * proc -- The various actively and passively monitored
               processes running on the MGC. Use the RTRV-SOFTW:ALL
               command to display all processes.
```

```
              * log level -- Sets the logging level for the specified
               process. Logging levels are as follows:
```

- CRIT -- Critical level messages.
- DEBUG -- Debug-level messages (lowest level).
- ERR -- Error condition messages.
- INFO -- Informational messages.
- WARN -- Warning condition messages.
- TRACE -- Trace messages.

```
Example:      The MML command shown in the following example retrieves
               the logging level of the ENG-01 process:
```

```
mml> RTRV-LOG:ENG-01
Media Gateway Controller - MGC-01 2000-01-16 09:38:03
M RTRV
"ENG-01:DEBUG"
;
```

```
Comments:     This command was introduced in Release 7.4. For
               information concerning backward compatibility, use the
               HELP:CHG-LOG command.
```

Note: DSKM-01, the disk monitor process, does not make use of log levels and therefore does not accept log-level change requests.

To display information on all of the MML commands, log in to the active Cisco MGC, start an MML session, and enter the following command:

help

The system returns a response similar to the following:

```
MGC-01 - Media Gateway Controller 2001-06-12 14:37:34
M   RTRV
```

```
Available commands (in alphabetical order):
ack-alm:<comp>:"<alm cat>"      Acknowledges an alarm category on a
                                component
blk-cic:<ptcode>:CIC=<number>[,RNG=<slaves>]
                                Blocks a circuit or a circuit range
chg-dpl::CUSTGRPID="<customer group ID>"
                                Reloads a dialing plan
chg-log:<proc>:<log level>      This command has been replaced by
                                set-log. Please refer to help on
                                set-log for further information
clr-alm:<comp>:"<alm cat>"      Clears an alarm category on a
                                component
clr-meas:<comp>:"<meas cat>"    Resets a measurement category on a
                                component
clr-tcap-trans::T=<number>      Clears all TCAP transactions
                                older than value of T in seconds
diaglog:<file name>:START|STOP  Starts/stops diagnostics log
h[:<number>[,<number>]]        Displays a history of commands for a
                                specified backward number or range;
                                the last command by default
help[:<command name>]          Displays the list of MML commands or
                                the help information on a specified
                                command
numan-add:<comp>:custgrpid=<cust group ID>,<param name>=<param value>,...
                                Adds an element to a dial plan table
numan-dlt:<comp>:custgrpid=<cust group ID>
                                Deletes an element from a dial plan
                                table
numan-ed:<comp>:custgrpid=<cust group ID>,<param name>=<param value>,...
                                Edits an element in a dial plan table
numan-rtrv:<comp>:custgrpid=<cust group ID>
                                Retrieves an element from a dial plan
                                table
numan-rtrv:<comp>:custgrpid=<cust group ID>,"all"
                                Retrieves all elements from a dial plan
                                table
prov-add:<comp>:name=<MML name>,<param name>=<param value>,...
                                Adds the component
prov-cpy                        Commits provisioning data
prov-dlt:<comp>:name=<MML name>  Deletes the component
prov-dply                      Deploys provisioning data
prov-ed:<comp>:name=<MML name>,<param name>=<param value>,...
                                Modifies the component attributes
prov-exp:<tid>:dirname="<export directory name>"
                                Exports provisioning data to the given
                                export directory name
                                tid can be one of the following:
                                    all
                                    config
```

```

trunk
trkgrp
numan
routing
export directory name can be any
directory name, in double quotes,
which will be created under the
cust_specific directory
prov-rtrv:<comp>:name=<MML name> Retrieves the component attributes
prov-rtrv:all Retrieves all the components
prov-rtrv:rttrnkgrp:"all" Retrieves all route trunk group
information
prov-rtrv:rttrnk:"all" Retrieves all route trunk information
prov-rtrv:rtlist:"all" Retrieves all route list information
prov-rtrv:session Retrieves provisioning session
information if one exists
prov-rtrv:variants Retrieves all variants
prov-sta::srcver=<version>,dstver=<version>
prov-stp Starts a provisioning session
Stops the current provisioning
session
prov-stp:<session name>:confirm Stops the specified provisioning
session
prov-sync Synchronizes provisioning data
prt-call:<sig path>|<trk grp>:[CIC=<number>|SPAN=<number>[BC=<number>]]
[,LOG=<logname>] [,EVT]
Prints diagnostic information about an
active call into the log file
query-cic:<ptcode>:CIC=<number>[,RNG=<slaves>][,RSLV]
Performs a circuit query for a circuit
or a circuit range with an optional
RESOLVE parameter
quit Ends the session
r[:<number>] Repeats a previously entered command
with a specified backward number;
the last command by default
reset-cic:<ptcode>:CIC=<number>[,RNG=<slaves>]
Resets a circuit or a circuit range
rtrv-admin-state:<target>:<param>
Retrieves the administrative state
of the target;
target can be a MGC or gateway or
trunk group or sigPath;
param can be one of the following
combinations:
[span=number] or
[span=number,]bc=number[,RNG=number]
or
cic=number[,RNG=number]
rtrv-alms Displays all active alarms
rtrv-alms::CONT Displays all active alarms and listens
for alarm events until Ctrl-C
rtrv-aud-gw:<sig path MGCP> Retrieves result of an auditing process
of a gateway
rtrv-aud-gw:all Retrieves results of auditing processes
of all gateways
rtrv-cfg:<cfg table> Displays contents of a configuration
table where table can be:
alarmCategories | components |
componentTypes | measCategories |
services | tables
rtrv-cic:<ptcode>:CIC=<number>[,RNG=<slaves>]
Retrieves bearer channels of a point
code

```

| | |
|--|---|
| rtrv-ctr:<comp>:"<meas cat>" | Retrieves a measurement of a component |
| rtrv-dest:<path> | Retrieves state of a destination,
<path> is one of the following:
<eisuppath> <faspath> <ipfaspath>
<naspath> <tcapippath>
<ptcode(destination only)> |
| rtrv-dest:all | Retrieves state of all destinations |
| rtrv-lnk-ctr:<C7 link/set> | Retrieves all measurements of a link or
link set |
| rtrv-lnk-ctr:all | Retrieves all measurements of all links |
| rtrv-log:all | Displays logging level of all processes |
| rtrv-log:<proc> | Displays logging level of a process |
| rtrv-lset:<C7 link set> | Displays state of a link set |
| rtrv-lssn:all | Displays state of local SSN |
| rtrv-mml | Displays all active MML sessions |
| rtrv-ne | Displays attributes of the Network
Element |
| rtrv-ovld | Displays overload level and number of
messages in a queue |
| rtrv-rssn:all | Displays state of remote SSN |
| rtrv-rte:<ptcode> | Retrieves all SS7 routes for a point
code |
| rtrv-rte:all | Retrieves SS7 routes for all point
codes |
| rtrv-sc:<c7iplnk> <tdmlnk> <iplnk> | Displays attributes of a signaling
channel |
| rtrv-sc:<lnkset> | Displays attributes of a link set |
| rtrv-sc:all | Displays attributes of all signaling
channels and link sets |
| rtrv-sc-trc | Displays the names of all files
currently open for the various traces
in progress |
| rtrv-softw:<proc> | Displays status of a process or
process group |
| rtrv-softw:all | Displays status of all known processes |
| rtrv-sp-ctr:<ptcode> | Retrieves all measurements of a point
code |
| rtrv-sp-ctr:all | Retrieves all measurements of all point
codes |
| rtrv-spc:<ptcode> | Retrieves route set of a point code |
| rtrv-spc:all | Retrieves route sets of all point codes |
| rtrv-ss7-slt:<C7 link> | Retrieves result of an MTP SLT test on
a link |
| rtrv-ss7-srt:<ptcode>:LSET="<C7 link/set>" | Retrieves result of an MTP SRT test on
a point code |
| rtrv-tc:<sig path>&<sig path>... | Displays state of bearers per signaling
path(s) |
| rtrv-tc:all | Displays state of all bearers |
| rtrv-tc-held:<sig path>&<sig path>... | Displays state of bearers per signaling
path(s) held by gateway |
| rtrv-tc-held:all | Displays state of all bearers, held by
gateway |
| rtrv-tcap-trans | Displays number of active TCAP
transactions |
| set-admin-state:<target>:<param>,LOCK UNLOCK RESET | Sets the administrative state of
the target;
target can be a MGC or gateway or
trunk group or sigPath;
param can be one of the following
combinations:
[span=number] or |

| | |
|---|--|
| | [span=number,]bc=number[,RNG=number]
or
cic=number[,RNG=number]
Changes service state of an ASP |
| set-dest-state:<path>:IS OOS | Changes service state of a destination,
<path> is one of the following:
<eisuppath> <faspath> <ipfaspath>
<naspath> <tcapippath>
<ptcode(destination only)> |
| set-lnk-state:<c7iplnk> <tdmlnk (c7 only)> <lnkset>:IS OOS FOOS INH UNH | Changes service state of a link or a
linkset |
| set-log:<proc>:<log level> | Sets logging level for process <proc> |
| set-log:all:<log level> | Sets logging level for all processes. |
| set-log:<proc>:debug,confirm | Sets debug logging level for <proc>
logLevel can be:
DEBUG TRACE INFO WARN ERR
CRIT
when setting to debug level, the confirm
parameter is mandatory |
| set-lssn-state:<SSN>:IS OOS | Changes service state of a local SSN |
| set-sc-state:<c7iplnk> <tdmlnk> <iplnk(non-NAS)>:IS OOS | Changes service state of a signaling channel |
| set-spc-state:<ptcode>:IS OOS... | Changes service state of a point code |
| snd:ext:<string> | Sends a message to an external process |
| snd:ext:"help" | Displays a list of commands available
for an external process (provided
by external process, not MML) |
| sta-aud | Starts auditing process |
| sta-aud-gw:<sig path MGCP> | Starts auditing process of a gateway |
| sta-aud-gw:all | Starts auditing processes of all
gateways |
| sta-abn-trc:<sig path> all:params | Starts dumping diagnostic info for
abnormally terminated calls on entire
MGC or a specified signal path or a
point code ,
optional params are:
CONFIRM - confirms tracing over all or
signal path or point code
(not needed when using span or
trunk - otherwise required)
log="filename" output file name in
the ../var/trace directory
span=x, where x is the span number of
interest
trk=y, where y is the trunk number
tc=c, where c is the traffic channel
of interest
rng=b, where b is the range of spans
prd=n, where n is the period in
seconds that this trace needs to be
run for (default is half minutes or
30 seconds) |
| sta-sc-trc:<sig path> <trkgrp>:params | Starts tracing on a signal path or a
point code or a trunk group,
optional params are:
CONFIRM - confirms tracing over a
signal path or point code or trunk
group (not needed when using span or
trunk - otherwise required) |

| | |
|--|---|
| | log="filename" output file name in the ../var/trace directory |
| | span=x, where x is the span number of interest |
| | trk=y, where y is the trunk number |
| | tc=c, where c is the traffic channel of interest |
| | rng=b, where b is the range of spans |
| | prd=n, where n is the period in seconds that this trace needs to be run for (default is 30 minutes or 1800 seconds) |
| sta-softw:<proc> | Starts a process or process group |
| sta-ss7-slt:<C7 link> | Starts an MTP SLT test on a link |
| sta-ss7-srt:<ptcode>:LSET="<C7 link/set>" | Starts an MTP SRT test on a point code |
| sta-tcap-trc | Starts TCAP tracing |
| stp-abn-trc:<sig path> <trkgrp> | Stops abnormal tracing on a signal path |
| stp-abn-trc:all | Stops abnormal tracing on all signal paths |
| stp-aud | Stops auditing process |
| stp-call:<target>:<param> | Stops call(s) in progress for the given target;
target can be a MGC or gateway or trunk group or sigPath;
param can be one of the following combinations:
[span=number,]confirm or
[span=number,]bc=number,[RNG=number,]confirm or
cic=number,[RNG=number,]confirm |
| stp-sc-trc:<sig path> <trkgrp> | Stops tracing on a signal path or trunk group |
| stp-sc-trc:all | Stops tracing on all signal paths |
| stp-softw:<proc>:[kill] | Stops a process or all processes in a group |
| stp-softw:all:[kill] | Shuts down the platform and applications except Process Manager |
| stp-tcap-trc | Stops TCAP tracing |
| sw-over::CONFIRM | Forces a switchover to a stand-by platform |
| tst-cot:<ptcode>:CIC=<number> | Performs a COT test on a circuit |
| unblk-cic:<ptcode>:CIC=<number>[,RNG=<slaves>] | Unblocks a circuit or a circuit range |
| vld-cic:<ptcode>:CIC=<number> | Performs a circuit validation |

Reentering Previously Entered MML Commands

You can use the **r** MML command reenter an MML command, either a specific MML command or the last MML command you entered.

To reenter the last MML command entered, log in to the active Cisco MGC, start an MML session, and enter the following command:

```
r
```

The system returns a response appropriate to the previously entered command. For example, if the previously entered command was **rtrv-spc:all**, a response similar to the following would be returned:

```
MGC-01 - Media Gateway Controller 2001-06-08 10:20:38
M  RTRV
    "dpc1:DPC=244.001.040,DNW=2:OPC=244.001.004:IS"
    "dpc2:DPC=244.001.041,DNW=2:OPC=244.001.004:IS"
    "dpc4:DPC=244.001.044,DNW=2:OPC=244.001.004:AOOS"
```

```
"dpc5:DPC=244.001.045,DNW=2:OPC=244.001.004:AOOS"  
"dpc8:DPC=244.018.030,DNW=2:OPC=244.001.004:AOOS"  
"dpc9:DPC=244.018.031,DNW=2:OPC=244.001.004:AOOS"  
"dpc10:DPC=244.018.032,DNW=2:OPC=244.001.004:AOOS"  
"dpc11:DPC=244.018.033,DNW=2:OPC=244.001.004:AOOS"
```

To reenter a particular MML command that you entered, log in to the active Cisco MGC, start an MML session, and enter the following command:

```
r::number
```

Where *number* is the number of the MML command you want to reenter. The last MML command you entered is equal to 1, the command you entered before that would be equal to 2, and so on.

For example, to reenter the tenth most recently entered MML command, you would enter the following command:

```
r::10
```

The system returns a response appropriate to the previously entered command.

Retrieving Active MML Sessions

To retrieve information on the active MML sessions, log in to the active Cisco MGC, start an MML session, and enter the following command:

```
rtrv-mml
```

The system returns a response similar to the following:

```
Media Gateway Controller - MGC-01 2000-01-12 15:19:51  
M RTRV  
mml5:guest
```

The response lists the session number (mml5 in the example) and the user ID of the session owner (guest in the example).

Ending an MML Session

You can use the **quit** MML command to end your current MML session.

Managing Signaling Channels

The operations you can use to manage an MML session are described in the following sections:

- Retrieving Signaling Channel Attributes, page 3-48
- Retrieving Signaling Destination Service States, page 3-50
- Retrieving the Service State of a Linkset, page 3-51
- Retrieving the State of SS7 Routes, page 3-52
- Retrieving the State of All Local Subsystem Numbers, page 3-53
- Retrieving the State of All Remote Subsystem Numbers, page 3-53
- Clearing TCAP Transactions, page 3-54
- Enabling Group Service Reset Messages, page 3-55

- Enabling Blocking/Unblocking Messages, page 3-54

Retrieving Signaling Channel Attributes

You can retrieve attributes for an individual signaling channel or linkset, or for all signaling channels and linksets.

To retrieve the attributes for an individual signaling channel or linkset, log in to the active Cisco MGC, start an MML session, and enter the following command:

```
rtrv-sc:sig_channel | linkset
```

Where:

- *sig_channel*—The MML name of a provisioning component, TDM link, C7 IP link, or IP link.
- *linkset*—The MML name of a linkset.

For example, to retrieve attributes for a signaling channel called iplink1, enter the following command:

```
rtrv-sc:iplink1
```

The system returns a response similar to the following:

```
Media Gateway Controller 2000-03-26 20:26:18
M RTRV
"iplink1:nassvc1,LID=0:IS"
```

To retrieve attributes for all of the signaling channels and linksets, log in to the active Cisco MGC, start an MML session, and enter the following command:

```
rtrv-sc:all
```

The system returns a response similar to the following, which shows the signaling links to and from the Cisco MGCs and the associated media gateways (different SS7 solutions might use different 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 */
```



Note

If a signaling channel is in a state other than IS, attempt to bring it into service, as described in the “Setting the Service State of a Signaling Channel” section on page 8-58

Understanding Signaling Channels

Signaling channels are bidirectional transport mechanisms for call-control signaling between the Cisco MGC and other devices, such as the Cisco SLTs, that provide necessary delivery reliability for higher-layer protocols. All types of signaling channels have basically the same functionality and are managed similarly. Unless otherwise noted, all commands, counters, and alarms apply to all types of signaling channels.

The basic types of signaling channels on the Cisco MGC are

- SS7 Message Transfer Part (MTP)—Used for reliable delivery. MTP level 2 provides point-to-point delivery. MTP level 3 maintains multiple load-sharing links and multiple routes between SS7 point codes.
- SS7 MTP over IP (SS7/IP)—MTP level 2 is terminated on the Cisco SLT. MTP level 3 is backhauled to the Cisco MGC by means of the Cisco-proprietary Reliable User Datagram Protocol (RUDP).
- Facility Associated Signaling (FAS)—Found in ISDN PRI or DPNSS over a 64-Kbps channel. Reliable delivery is provided by some form of Link Access Protocol (LAP), for example Q.921.
- FAS over IP (FAS/IP)—Same as FAS, but uses IP as its transport mechanism. Reliable delivery is provided by Q.921 LAP-D or RUDP/SM.
- Media Gateway Control Protocol (MGCP)—Reliable delivery is also provided by the MGCP, which uses UDP/IP.

The following sections describe the information returned by the system when you enter the **rtv-sc** MML command.

Signaling channel or linkset name

The first field lists the MML name of the signaling channel or linkset.

Parent Name

The second field lists the MML name of the parent of the signaling channel or linkset.

Link ID

The LID field lists the associated link identification number.

Subsystem Number

The SSN field lists the associated subsystem number.

Primary Service State

The PST field shows the current primary service state of the destination. Table 3-8 lists the valid primary service state values:

Table 3-8 Signaling Channel Primary Service States

| Link State ID | Link State | Description |
|---------------|------------------------------|---|
| AOOS | Automatically out-of-service | The system has taken the signaling channel out-of-service (OOS). |
| INB | Install busy | When a system is first configured, all signaling links default to this state and must be manually set in-service (IS) through the use of the set-sc-state MML command. |
| IS | In-service | The signaling channel is IS and fully operational. This is its normal operating state. |
| MOOS | Manually out-of-service | The signaling channel has been manually taken OOS. |

Table 3-8 *Signaling Channel Primary Service States (continued)*

| Link State ID | Link State | Description |
|---------------|----------------|---|
| OOS | Out-of-service | The signaling channel is OOS from the remote end. The system is actively trying to restore the signaling channel. |
| TRNS | Transient | The state of the signaling channel is currently being changed. |
| UNK | Unknown | The state of the signaling channel is not known. |

Secondary Service State

The SST field shows the current secondary service state of the specified signaling channel. The valid states are listed below:

- ACKD—SS7 Acknowledgement delay
- BSNR—SS7 backward sequence number received (BSNR)
- CIS—Commanded in service
- CONF—Configuration failure
- COOS—Commanded out of service
- ENGR—Call engine reset
- ISPEND—In service, pending
- LCNG—Congestion, local
- LINE—Line failure
- LINH—SS7 local inhibit
- LINK—Link failure
- LINS—Linkset failure
- NA—Cause not available
- OOSPEND—Out of service, pending
- PRHB—SS7 prohibited
- RBLK—SS7 remote blocked
- RCNG—Congestion, remote
- RINH—SS7 remote inhibit
- RSTR—SS7 restricted
- SERR—SS7 signal error
- STBY—Cause standby
- SUPPENT—Supporting entity
- TPATH—Traffic path
- UNK—Cause unknown

Retrieving Signaling Destination Service States

Retrieving state information about all external point codes and signal paths is a task that performed daily. For more information about this and other daily task refer to the “Daily Tasks” section on page 3-1.

To retrieve information about a specific DPC or non-ISUP signaling service, log in to the active Cisco MGC, start an MML session, and enter the following command:

```
rtrv-dest: point_code | sig_srv
```

Where:

- *point_code*—The MML name of the DPC.
- *sig_srv*—The MML name of the non-ISUP signaling service.

The system returns a response similar to the following:

```
MGC-01 - Media Gateway Controller 2001-06-12 14:53:03
M  RTRV
    "dpc1:PKG=SS7-ANSI,ASSOC=SWITCHED,PST=IS,SST=RCNG"
```

For more information on the response to this command, refer to the “Understanding the Destination State Information” section on page 3-9.

If the destination is in a primary service state other than IS, attempt to bring it into service, as described in the “Setting the Service State of a Destination” section on page 8-59



Note

If the **rtrv-dest** MML command is entered 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 Cisco MGC has not received a service state message from the associated destination since the switchover occurred. No user action is required.

Retrieving the Service State of a Linkset

To retrieve the service state of a linkset, log in to the active Cisco MGC, start an MML session, and enter the following command:

```
rtrv-lset: linkset
```

Where *linkset* is the MML name of the desired linkset.

For example, to retrieve the service state of a linkset called ls1, you would enter the following command:

```
rtrv-lset: ls1
```

The system returns a response similar to the following:

```
Media Gateway Controller - MGC-01 2000-01-12 15:19:51
M  RTRV
    IS
```

The valid service states for a linkset are identical to the primary service state listings for signaling channels, as found in the “Understanding Signaling Channels” section on page 3-48. If the linkset is in any other state than IS, attempt to bring the linkset into service, as described in the “Setting the Service State of a Link or Linkset” section on page 8-60.

Retrieving the State of Point Codes

To retrieve the current state for the route set for one point code, log in to the active Cisco MGC, start an MML session, and enter the following command:

```
rtrv-spc: point_code
```

Where *point_code* is the MML name for the associated point code.

The system returns a response similar to the following:

```
MGC-01 - Media Gateway Controller 2001-06-12 16:10:21
M RTRV
"dpc1:DPC=244.001.040,DNW=2:OPC=244.001.004:AOOS"
```

To retrieve the current state for the route sets for all point codes, log in to the active Cisco MGC, start an MML session, and enter the following command:

```
rtrv-spc:all
```

The system returns a response similar to the following:

```
MGC-01 - Media Gateway Controller 2001-06-12 16:04:59
M RTRV
"dpc1:DPC=244.001.040,DNW=2:OPC=244.001.004:IS"
"dpc2:DPC=244.001.041,DNW=2:OPC=244.001.004:IS"
"dpc4:DPC=244.001.044,DNW=2:OPC=244.001.004:IS"
"dpc5:DPC=244.001.045,DNW=2:OPC=244.001.004:IS"
"dpc8:DPC=244.018.030,DNW=2:OPC=244.001.004:IS"
"dpc9:DPC=244.018.031,DNW=2:OPC=244.001.004:IS"
"dpc10:DPC=244.018.032,DNW=2:OPC=244.001.004:IS"
"dpc11:DPC=244.018.033,DNW=2:OPC=244.001.004:IS"
```

The valid service states for a linkset are identical to the primary service state listings for signaling channels, as found in the “Understanding Signaling Channels” section on page 3-48. If the linkset is in any other state than IS, attempt to bring the linkset into service, as described in the “Setting the Service State of a Signaling Point Code” section on page 8-60.

Retrieving the State of SS7 Routes

To retrieve the current state for an SS7 route, log in to the active Cisco MGC, start an MML session, and enter the following command:

```
rtrv-rte:point_code
```

Where *point_code* is the MML name for the associated point code.

The system returns a response similar to the following:

```
MGC-01 - Media Gateway Controller 2001-06-12 16:17:55
M RTRV
"dpc1:linkset1,APC=244.001.040,PRI0=1,PST=AOOS,SST=NA"
"dpc1:UNK,APC=000.000.000,PRI0=2,PST=IS,SST=NA"
```

To retrieve the current state for all of SS7 routes, log in to the active Cisco MGC, start an MML session, and enter the following command:

```
rtrv-rte:all
```

The system returns a response similar to the following:

```
MGC-01 - Media Gateway Controller 2001-06-12 16:15:51
M RTRV
"dpc1:linkset1,APC=244.001.040,PRI0=1,PST=AOOS,SST=NA"
"dpc1:UNK,APC=000.000.000,PRI0=2,PST=IS,SST=NA"
"dpc2:linkset2,APC=244.001.041,PRI0=1,PST=AOOS,SST=NA"
"dpc2:UNK,APC=000.000.000,PRI0=3,PST=IS,SST=NA"
"dpc4:linkset4,APC=244.001.044,PRI0=1,PST=AOOS,SST=NA"
"dpc4:UNK,APC=000.000.000,PRI0=4,PST=AOOS,SST=NA"
"dpc5:linkset5,APC=244.001.045,PRI0=1,PST=AOOS,SST=NA"
"dpc5:UNK,APC=000.000.000,PRI0=5,PST=AOOS,SST=NA"
```

```
"dpc8:linkset8,APC=244.018.030,PRI0=1,PST=AOOS,SST=NA"
"dpc8:UNK,APC=000.000.000,PRI0=6,PST=AOOS,SST=NA"
"dpc9:linkset9,APC=244.018.031,PRI0=1,PST=AOOS,SST=NA"
"dpc9:UNK,APC=000.000.000,PRI0=7,PST=AOOS,SST=NA"
"dpc10:linkset10,APC=244.018.032,PRI0=1,PST=AOOS,SST=NA"
"dpc10:UNK,APC=000.000.000,PRI0=8,PST=AOOS,SST=NA"
```

The valid service states for a linkset are identical to the primary service state listings for signaling channels, as found in the “Understanding Signaling Channels” section on page 3-48. If the linkset is in any other state than IS, attempt to bring the linkset into service, as described in the “Setting the Service State of a Destination” section on page 8-59.

Retrieving the State of All Local Subsystem Numbers

To retrieve the state of all local subsystem number (SSNs), log in to the active Cisco MGC, start an MML session, and enter the following command:

```
rtrv-lssn:all
```

The system returns a response similar to the following:

```
Media Gateway Controller - MGC-01 2000-01-12 15:19:51
M RTRV
  "TCAP-01:SSN=1,PST=IS"
  "TCAP-01:SSN=2,PST=OOS"
```

The response indicates the name of the associated process, the SSN, and the state (either in-service or out-of-service). If any of the local SSNs are out of service, proceed to the “Setting the Service State of a Local Subsystem Number” section on page 8-61.

Retrieving the State of All Remote Subsystem Numbers

To retrieve the state of all remote SSNs, log in to the active Cisco MGC, start an MML session, and enter the following command:

```
rtrv-rssn:all
```

The system returns a response similar to the following:

```
Media Gateway Controller - MGC-01 2000-01-12 15:19:51
M RTRV
  "stp1:PC=007.007.007,SSN=1,PST=OOS"
  "stp2:PC=008.008.008,SSN=1,PST=OOS"
  "stp3:PC=009.009.009,SSN=2,PST=OOS"
```

The response indicates the name of the associated process, the SSN, and the state (either in-service or out-of-service). If any of the remote SSNs are out of service, proceed to the “SS7 Network Related Problems” section on page 8-50.

Retrieving TCAP Transactions

To retrieve the number of active transaction capabilities application part (TCAP) transactions, log in to the active Cisco MGC, start an MML session, and enter the following command:

```
rtrv-tcap-trans
```

The system returns a response similar to the following:

```
Media Gateway Controller - MGC-01 2000-01-12 15:19:51
M   RTRV
    "TCAP-01:TRANS=0"
```

Clearing TCAP Transactions

To clear all TCAP transactions that are older than a period you specify, log in to the active Cisco MGC, start an MML session, and enter the following command:

```
clr-tcap-trans::t=number
```

Where *number* is the time period, in seconds, after which you want to clear TCAP transactions.

For example, to clear all TCAP transactions that are older than 60 seconds, you would enter the following command:

```
clr-tcap-trans::t=60
```

Enabling Blocking/Unblocking Messages

You may want to modify the properties of an IP FAS signaling service to enable your system to send blocking (BLO) and unblocking (UBL) messages when bearer channels go IS and OOS, respectively. The process of modifying the properties of a signaling service is referred to as dynamic reconfiguration. For more information about dynamic reconfiguration, refer to the “Understanding Dynamic Reconfiguration” section on page 3-66.



Caution

We do not recommend enabling the sending of BLO/UBL messages on your Cisco MGC.



Note

You can use the CMM or the VSPT to enable the sending of BLO/UBL messages on your system. Refer to the *Cisco Media Gateway Controller Software Release 7 Provisioning Guide* for more information about using the CMM or VSPT to modify the properties of an IP FAS signaling service.

To enable your system to send BLO and UBL messages, perform the following steps:

- Step 1** Start a provisioning session, as described in the “Starting a Provisioning Session” section on page 3-63.
- Step 2** Enter the following command to set the property that enables the sending of BLO/UBL messages when bearer channels go IS/OOS, respectively:

```
prov-ed:ipfaspath:name="comp_name",PropagateSvcMsgBlock=true
```

Where *comp_name* is the MML name for the IP FAS signaling service on which you are enabling BLO/UBL messages.

For example, to enable the sending of BLO/UBL messages on an IP FAS signaling service named **ipfas1**, you would enter the following command:

```
prov-ed:ipfaspath:name="ipfas1",PropagateSvcMsgBlock=true
```

- Step 3** Save and activate your provisioning changes, as described in the “Saving and Activating your Provisioning Changes” section on page 3-64.
-

Enabling Group Service Reset Messages

You may want to modify the properties of an SS7 signaling service to enable your system to send SS7 group service reset (GSR) messages for all CICs during point code initialization, so that the Cisco MGC to synchronize its bearer channel blocking state with that of the end office. The process of modifying the properties of a signaling service is referred to as dynamic reconfiguration. For more information about dynamic reconfiguration, refer to the “Understanding Dynamic Reconfiguration” section on page 3-66.



Caution

We do not recommend enabling the sending of GSR messages on your Cisco MGC.



Note

You can use the CMM or the VSPT to enable the sending of GSR messages on your system. Refer to the *Cisco Media Gateway Controller Software Release 7 Provisioning Guide* for more information about using the CMM or VSPT to modify the properties of an SS7 signaling service.

To enable the sending of GSR messages, perform the following steps:

- Step 1** Start a provisioning session as described in the “Starting a Provisioning Session” section on page 3-63.

- Step 2** Enter the following command to set the property that enables the sending of GRS messages for CICs during point code initialization:

```
prov-ed:ss7path:name="comp_name",GRSEnabled=true
```

Where: *comp_name*—MML name for the SS7 signaling service on which you are enabling the sending of GRS messages.

For example, to enable the sending of GRS messages on an SS7 signaling service named **ss7svc1**, you would enter the following command:

```
prov-ed:ss7path:name="ss7svc1",GRSEnabled=true
```

- Step 3** Save and activate your provisioning changes as described in the “Saving and Activating your Provisioning Changes” section on page 3-64.
-

Managing Bearer Channels

The operations you can use to manage bearer channels are described in the following sections:

- Verifying Proper Replication of Calls, page 3-56
- Retrieving the States of Bearers Held By a Media Gateway, page 3-57
- Blocking CICs, page 3-58
- Retrieving the Administrative State, page 3-59

Verifying Proper Replication of Calls

Ensure that the standby Cisco MGC becomes fully operational and that the replication of calls in progress has been completed by performing the steps in the following procedure:



Caution

The following command retrieves the current status of *all* provisioned traffic channels. If you have a large number of traffic channels, you might want to limit the command to a subset of the provisioned channels, perhaps on a signaling-service-by-signaling-service basis. For example, to see just the provisioned channels for a signaling service named `ss7svc2`, you would enter the following command: **`rtrv-tc:name="ss7svc2"`**.

Step 1 Log in to the active Cisco MGC, start an MML session, and enter the following command:

```
rtrv-tc:all
```

The system returns a different set of responses, depending on which release of the MGC software you are running and the type of configuration you are using on the associated media gateway.

When the Cisco MGC software is used on a nailed network, 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"
```

When the Cisco MGC software is used on a switched network, the system returns a response similar to the following:

```
Media Gateway Controller - MGC-04 2000-04-05 08:05:54
M RTRV
"dpc1:CIC=1,PST=IS,CALL=IDLE,GW_STAT=CNX_IS,BLK=NONE"
"dpc1:CIC=2,PST=IS,CALL=IDLE,GW_STAT=CNX_IS,BLK=NONE"
"dpc1:CIC=3,PST=IS,CALL=IDLE,GW_STAT=CNX_IS,BLK=NONE"
"dpc1:CIC=4,PST=IS,CALL=IDLE,GW_STAT=CNX_IS,BLK=NONE"
"dpc1:CIC=5,PST=IS,CALL=IDLE,GW_STAT=CNX_IS,BLK=NONE"
"dpc1:CIC=6,PST=IS,CALL=IDLE,GW_STAT=CNX_IS,BLK=NONE"
"dpc1:CIC=7,PST=IS,CALL=IDLE,GW_STAT=CNX_IS,BLK=NONE"
"dpc1:CIC=8,PST=IS,CALL=IDLE,GW_STAT=CNX_IS,BLK=NONE"
"dpc1:CIC=9,PST=IS,CALL=IDLE,GW_STAT=CNX_IS,BLK=NONE"
```



Note

An explanation of the fields in the response can be found in the “Understanding CIC States” section on page 3-14.

Step 2 Repeat Step 1 on the standby Cisco MGC.

Step 3 Verify that the CICs in both systems are in sync and show the same status. Calls in progress should say `CALL=IN` for both systems.

If necessary, you can force the active Cisco MGC to do a maintenance switchover (see the “Performing a Manual Switchover” section on page 3-80) and repeat the above procedure for that system.

Retrieving the States of Bearers Held By a Media Gateway

You can retrieve the states of bearer channels being held by a media gateway. To retrieve the state of a group bearer channels associated with one or more signaling destination(s) that are being held by a media gateway, log in to the active Cisco MGC, start an MML session, and enter the following command:

```
rtrv-tc-held:sig_dest| &sign_dest...
```

Where *sig_dest* is a logical signaling destination, such as an SS7 point code, FAS path, IP FAS path, or DPNSS path. You can display a complete list of configured components by performing the procedure in the “Retrieving component data” section on page 3-87.

When none of the group of bearer channels associated with the specified signaling destination(s) are being held by a media gateway, the system returns a response similar to the following:

```
MGC-01 - Media Gateway Controller 2001-06-12 16:28:39
M   RTRV
    "dpc1"
    /* No bearer channels in held state */
```

When bearer channels associated with the specified signaling destination(s) are being held by a media gateway, the system returns a response similar to the following:

```
MGC-01 - Media Gateway Controller 2001-06-12 16:28:39
M   RTRV
    "dpc1:CIC=1,PST=IS,CALL=IDLE,GW_STAT=CCN_IS,BLK=NONE"
    "dpc1:CIC=1,PST=IS,CALL=IDLE,GW_STAT=CCN_IS,BLK=NONE"
    "dpc1:CIC=2,PST=IS,CALL=IDLE,GW_STAT=CCN_IS,BLK=NONE"
    "dpc1:CIC=3,PST=IS,CALL=IDLE,GW_STAT=CCN_IS,BLK=NONE"
    "dpc1:CIC=4,PST=IS,CALL=IDLE,GW_STAT=CCN_IS,BLK=NONE"
    "dpc1:CIC=5,PST=IS,CALL=IDLE,GW_STAT=CCN_IS,BLK=NONE"
    "dpc1:CIC=6,PST=IS,CALL=IDLE,GW_STAT=CCN_IS,BLK=NONE"
    "dpc1:CIC=7,PST=IS,CALL=IDLE,GW_STAT=CCN_IS,BLK=NONE"
    "dpc1:CIC=8,PST=IS,CALL=IDLE,GW_STAT=CCN_IS,BLK=NONE"
    "dpc1:CIC=9,PST=IS,CALL=IDLE,GW_STAT=CCN_IS,BLK=NONE"
```

To retrieve the state of all bearer channels held by a media gateway, log in to the active Cisco MGC, start an MML session, and enter the following command:

```
rtrv-tc-held:all
```

When none of the bearer channels are being held by a media gateway, the system returns a response similar to the following:

```
Retrieving results. This could take a few moments...
MGC-01 - Media Gateway Controller 2001-06-12 16:28:39
M   RTRV
    "opc"
    /* No bearer channels in held state */
    "dpc1"
    /* No bearer channels in held state */
    "dpc2"
    /* No bearer channels in held state */
```

When bearer channels are being held by a media gateway, the system returns a response similar to the following:

```
MGC-01 - Media Gateway Controller 2001-06-12 16:28:39
M   RTRV
    "dpc1:CIC=1,PST=IS,CALL=IDLE,GW_STAT=CNX_IS,BLK=NONE"
    "dpc1:CIC=1,PST=IS,CALL=IDLE,GW_STAT=CNX_IS,BLK=NONE"
    "dpc1:CIC=2,PST=IS,CALL=IDLE,GW_STAT=CNX_IS,BLK=NONE"
    "dpc1:CIC=3,PST=IS,CALL=IDLE,GW_STAT=CNX_IS,BLK=NONE"
    "dpc1:CIC=4,PST=IS,CALL=IDLE,GW_STAT=CNX_IS,BLK=NONE"
    "dpc1:CIC=5,PST=IS,CALL=IDLE,GW_STAT=CNX_IS,BLK=NONE"
    "dpc1:CIC=6,PST=IS,CALL=IDLE,GW_STAT=CNX_IS,BLK=NONE"
    "dpc1:CIC=7,PST=IS,CALL=IDLE,GW_STAT=CNX_IS,BLK=NONE"
    "dpc1:CIC=8,PST=IS,CALL=IDLE,GW_STAT=CNX_IS,BLK=NONE"
    "dpc1:CIC=9,PST=IS,CALL=IDLE,GW_STAT=CNX_IS,BLK=NONE"
    "dpc2:CIC=10,PST=IS,CALL=IDLE,GW_STAT=CNX_IS,BLK=NONE"
    "dpc2:CIC=11,PST=IS,CALL=IDLE,GW_STAT=CNX_IS,BLK=NONE"
    "dpc2:CIC=12,PST=IS,CALL=IDLE,GW_STAT=CNX_IS,BLK=NONE"
    "dpc2:CIC=13,PST=IS,CALL=IDLE,GW_STAT=CNX_IS,BLK=NONE"
    "dpc2:CIC=14,PST=IS,CALL=IDLE,GW_STAT=CNX_IS,BLK=NONE"
    "dpc2:CIC=15,PST=IS,CALL=IDLE,GW_STAT=CNX_IS,BLK=NONE"
    "dpc2:CIC=16,PST=IS,CALL=IDLE,GW_STAT=CNX_IS,BLK=NONE"
    "dpc2:CIC=17,PST=IS,CALL=IDLE,GW_STAT=CNX_IS,BLK=NONE"
    "dpc2:CIC=18,PST=IS,CALL=IDLE,GW_STAT=CNX_IS,BLK=NONE"
```

Blocking CICs

You may need to block a CIC or a range of CICs on your Cisco MGC. Blocking a single CIC causes a BLA message to be sent to the destination SSP. Blocking a range of CICs causes a CGB message to be sent to the destination SSP. The range option only can be used to block CICs within a given trunk (T1 or E1).

To block a single CIC, log in to your active Cisco MGC, start an MML session and enter the following command:

```
blk-cic:dest_pc:CIC=number
```

Where:

- *dest_pc*—MML name of a DPC associated with the CIC you want to block.
- *number*—The number of the CIC you want to block.

For example, to block CIC number 1, which is associated with a DPC called dpc1, you would enter the following command:

```
blk-cic:dpc1:cic=1
```

To block a range of CICs, log in to your active Cisco MGC, start an MML session, and enter the following command:

```
blk-cic:dest_pc:CIC=number,RNG=range
```

Where:

- *point_code*—MML name of a DPC associated with the CICs you want to block.
- *number*—The number of the first CIC in the range of CICs you want to block.
- *range*—Specifies the end of the range of CICs to be blocked.

**Note**

The Cisco MGC software can be configured to issue individual or group supervision messages for point codes that are associated with an ISUP signaling service. ISUP signaling services issue group supervision messages by default. If an ISUP signaling service is configured to issue individual supervision messages, the *range* option cannot be used with this command. Blocking of CICs can only be done one CIC number at a time for point codes associated with an ISUP signaling service.

For example, to block CIC number 1 through 20, which are associated with a DPC called *dpc1*, you would enter the following command:

```
blk-cic:dpc1:cic=1, rng=20
```

To verify that the CIC(s) have been successfully blocked, retrieve the status of the affected CICs as described in the “Verifying CIC States” section on page 3-13. When you want to return the CIC(s) to service, you must unblock the CIC(s) as described in the “Unblocking CICs” section on page 8-86.

Retrieving the Administrative State

The administrative state refers to the state of CICs (on the Cisco MGC) and spans and bearer channels (on the associated media gateway). There are three possible states: locked, unlocked, and shutdown. You can use the **rtrv-admin-state** MML command to determine the administrative state of several objects in the Cisco SS7 solution environment, including the Cisco MGC, an associated MGCP media gateway, a trunk group, a signaling service, spans and bearer channels associated with a signaling service (for non-ISUP trunks), and CICs associated with a signaling service (for ISPU trunks).

When you retrieve the administrative state of a object that consists of groups of CICs or spans and bearer channels, you receive an inferred target state, based on the following criteria:

- If all circuits are in a locked state, the inferred target administrative state is locked.
- If at least one circuit is in an unlocked state, the inferred target administrative state is unlocked.
- If the circuits are in a mixture of the locked and shutdown states, the inferred target administrative state is shut down.

If you want to change the administrative state of a component, refer to the “Setting the Administrative State” section on page 8-70.

The following procedures describe how you can use the **rtrv-admin-state** MML command:

- Retrieving the Administrative State of a Cisco MGC, page 3-59
- Retrieving the Administrative State of a Media Gateway, page 3-60
- Retrieving the Administrative State of a Trunk Group, page 3-60
- Retrieving the Administrative State of a Signaling Service, page 3-60
- Retrieving the Administrative State of Spans, page 3-61
- Retrieving the Administrative State of CICs, page 3-62

Retrieving the Administrative State of a Cisco MGC

To retrieve the administrative state of a Cisco MGC, log in to the active Cisco MGC, start an MML session, and enter the following command:

```
rtrv-admin-state:mgc
```

Where *mgc* is the MML name of the Cisco MGC host.

The system returns a response similar to the following:

```
Media Gateway Controller - MGC-03 2000-02-17 14:27:52
M  COMPLD
   "mgca:PST=UNLOCK,LOCK=0,UNLOCK=384,SHUTDOWN=0"
```

If you want to change the administrative state of the Cisco MGC, refer to the “Setting the Administrative State of a Cisco MGC” section on page 8-71.

Retrieving the Administrative State of a Media Gateway

To retrieve the administrative state of an associated media gateway, log in to the active Cisco MGC, start an MML session, and enter the following command:

```
rtrv-admin-state:gateway
```

Where *gateway* is the MML name of the associated media gateway.

**Note**

Not all media gateway types are applicable. Supported types are CU, MUX, and MGW external nodes.

The system returns a response similar to the following:

```
Media Gateway Controller - MGC-03 2000-02-17 14:27:52
M  COMPLD
   "mgw1:PST=UNLOCK,LOCK=0,UNLOCK=384,SHUTDOWN=0"
```

If you want to change the administrative state of the media gateway, refer to the “Setting the Administrative State of a Media Gateway” section on page 8-71.

Retrieving the Administrative State of a Trunk Group

To retrieve the administrative state of a trunk group, log in to the active Cisco MGC, start an MML session, and enter the following command:

```
rtrv-admin-state:trkgrp
```

Where *trkgrp* is the MML name of the trunk group.

**Note**

This command can only be used for time-division multiplexing (TDM) trunk groups. Allow the corresponding MML name for component type "0020".

The system returns a response similar to the following:

```
Media Gateway Controller - MGC-03 2000-02-17 14:27:52
M  COMPLD
   "trunkgrp1:PST=UNLOCK,LOCK=0,UNLOCK=384,SHUTDOWN=0"
```

If you want to change the administrative state of the trunk group, refer to the “Setting the Administrative State of a Trunk Group” section on page 8-72.

Retrieving the Administrative State of a Signaling Service

To retrieve the administrative state of a signaling service, log in to the active Cisco MGC, start an MML session, and enter the following command:

```
rtrv-admin-state:sig_srv
```

Where *sig_srv* is the MML name of the signaling service. The following signaling service types are valid for this command:

- For in-band TDM up to MUX and then time switched to TDM media and sent to the Cisco MGC.
- For in-band TDM signaling up to CU and then encapsulated and sent over IP to the Cisco MGC.
- For in-band TDM signaling up to the media gateway and then converted to NI2 and sent to the Cisco MGC over IP (that is, FE box<-sig/tdm->media gateway<-NI2/IP-> Cisco MGC).
- Signaling service or routeset associated with a DPC.
- EISUP signaling service.

The system returns a response similar to the following:

```
Media Gateway Controller - MGC-03 2000-02-17 14:27:52
M  COMPLD
    "ss7svc1:PST=UNLOCK,LOCK=0,UNLOCK=384,SHUTDOWN=0"
```

If you want to change the administrative state of the signaling service, refer to the “Setting the Administrative State of a Signaling Service” section on page 8-73.

Retrieving the Administrative State of Spans

To retrieve the administrative state of a single span, log in to the active Cisco MGC, start an MML session, and enter the following command:

```
rtrv-admin-state:sig_srv,span=x
```

Where:

- *sig_srv* is the MML name of the signaling service. The following signaling service types are valid for this command:
 - For in-band TDM up to MUX and then time switched to TDM media and sent to the Cisco MGC.
 - For in-band TDM signaling up to CU and then encapsulated and sent over IP to the Cisco MGC.
 - For in-band TDM signaling up to the media gateway and then converted to NI2 and sent to the Cisco MGC over IP (that is, FE box<-sig/tdm->media gateway<-NI2/IP-> Cisco MGC).
 - Signaling service or routeset associated with a DPC.
 - EISUP signaling service.
- *x*—A16-bit value that identifies an ISDN/PRI physical cable.

For example, to determine the administrative state of span number 2 associated with a signaling service called ss7svc1, you would enter the following command:

```
rtrv-admin-state:ss7svc1,span=2
```

The system returns a response similar to the following:

```
Media Gateway Controller - MGC-03 2000-02-17 14:27:52
M  COMPLD
    "ss7svc1:PST=UNLOCK,LOCK=0,UNLOCK=384,SHUTDOWN=0"
```

To retrieve the administrative state of a bearer channel or a range of bearer channels in a span, log in to the active Cisco MGC, start an MML session, and enter the following command:

```
rtrv-admin-state:sig_srv,span=x,bc=y[,rng=range]
```

Where:

- *sig_srv* is the MML name of the signaling service. The following signaling service types are valid for this command:
 - For in-band TDM up to MUX and then time switched to TDM media and sent to the Cisco MGC.
 - For in-band TDM signaling up to CU and then encapsulated and sent over IP to the Cisco MGC.
 - For in-band TDM signaling up to the media gateway and then converted to NI2 and sent to the Cisco MGC over IP (that is, FE box<-sig/tdm->media gateway<-NI2/IP-> Cisco MGC).
 - Signaling service or routeset associated with a DPC.
 - EISUP signaling service.
- *x*—A 16-bit value that identifies an ISDN/PRI physical cable.
- *y*—A numeric value that identifies the non-ISUP bearer channel number.
- *range*—A value such that *y+range* is a valid bearer channel number. The administrative state for all bearer channels between *y* and *y+range* are retrieved.

For example, to determine the administrative state of bearer channels numbers 2 through 6, associated with a signaling service called *ss7svc1*, you would enter the following command:

```
rtrv-admin-state:ss7svc1,span=2,bc=2,rng=5
```

The system returns a response similar to the following:

```
Media Gateway Controller - MGC-03 2000-02-17 14:27:52
M COMPLD
"ss7svc1:PST=UNLOCK,LOCK=0,UNLOCK=384,SHUTDOWN=0"
```

If you want to change the administrative state of the spans, refer to the “Setting the Administrative State of Spans” section on page 8-73.

Retrieving the Administrative State of CICs

To retrieve the administrative state of a CIC or a range of CICs, log in to the active Cisco MGC, start an MML session, and enter the following command:

```
rtrv-admin-state:sig_srv,cic=number[,rng=range]
```

Where:

- *sig_srv* is the MML name of the signaling service. The following signaling service types are valid for this command:
 - For in-band TDM up to MUX and then time switched to TDM media and sent to the Cisco MGC.
 - For in-band TDM signaling up to CU and then encapsulated and sent over IP to the Cisco MGC.
 - For in-band TDM signaling up to the media gateway and then converted to NI2 and sent to the Cisco MGC over IP (that is, FE box<-sig/tdm->media gateway<-NI2/IP-> Cisco MGC).
 - Signaling service or routeset associated with a DPC.
 - EISUP signaling service.
- *number*—A valid CIC number.
- *range*—A value such that *y+range* is a valid CIC number. The administrative state for all CICs between *y* and *y+range* are retrieved.

For example, to determine the administrative state of CICs 2 through 11 associated with a signaling service called `ss7svc1`, you would enter the following command:

```
rtrv-admin-state:ss7svc1,cic=2,rng=9
```

The system returns a response similar to the following:

```
Media Gateway Controller - MGC-03 2000-02-17 14:27:52
M   COMPLD
    "ss7svc1:PST=UNLOCK,LOCK=0,UNLOCK=384,SHUTDOWN=0"
```

If you want to change the administrative state of the CICs, refer to the “Setting the Administrative State of CICs” section on page 8-75.

Provisioning your Cisco MGC

The operations you can use to provision your Cisco MGC are described in the following sections:

- Starting a Provisioning Session, page 3-63
- Saving and Activating your Provisioning Changes, page 3-64
- Ending a Provisioning Session Without Activating your Changes, page 3-65
- Invoking Dynamic Reconfiguration, page 3-65
- Retrieving Provisioning Data, page 3-67
- Provisioning a Dial Plan, page 3-73
- Importing Provisioning Data, page 3-73
- Exporting Provisioning Data, page 3-74
- Managing Automatic Congestion Control, page 3-75

For more detailed information about provisioning your Cisco MGC, refer to the *Cisco Media Gateway Controller Software Release 7 Provisioning Guide*.

Starting a Provisioning Session

You may need to start a provisioning session as part of your system operations. To do this, log into the active Cisco MGC, start an MML session, and enter the following command:

```
prov-sta::srcver="curr_ver",dstver="mod_ver"
```

Where:

- *curr_ver*—The name of the current configuration version. In place of the name of the current configuration version, you can also enter:
 - *new*—A new default session configuration; no existing source configuration is available.
 - *active*—Selects the active configuration as the source for configuration changes.



Note

If you do not know the name of your current configuration session, you can use the CONFIG-LIB viewer in the MGC toolbar to determine that name. For more information on the CONFIG-LIB viewer, proceed to the “Using the Config-Lib Viewer” section on page 3-113.

- *mod_ver*—A new configuration version name that contains your provisioning changes.

For example, to use a configuration version called **ver1** as the basis for a version to be called **ver2**, you would enter the following command:

```
prov-sta::srcver="ver1",dstver="ver2"
```

Once a provisioning session is underway, you may use the **prov-add**, **prov-ed**, or **prov-dlt** MML commands to add, modify, and delete components on your system. If you want to add components to your system, refer to the *Cisco Media Gateway Controller Software Release 7 Provisioning Guide*. If you want to modify or delete components on your system, refer to the “Invoking Dynamic Reconfiguration” section on page 3-65.

There are two ways to close your provisioning session: saving and activating your provisioning changes, as described in the “Saving and Activating your Provisioning Changes” section on page 3-64 or ending your provisioning session without saving and activating your changes, as described in the “Ending a Provisioning Session Without Activating your Changes” section on page 3-65.

Saving and Activating your Provisioning Changes

When you have completed making provisioning changes in your session, you must enter a command to save and activate your changes. There are two different provisioning MML commands that do this: **prov-cpy** and **prov-dply**.



Caution

Using the **prov-cpy** and **prov-dply** MML commands can severely impact your system’s call processing performance, depending on the extent of your provisioning changes. We recommend that these commands be issued during a maintenance window when traffic is minimal.

The **prov-cpy** MML command is used to save and activate your changes on the active Cisco MGC. This command is typically used to save and activate changes on a Cisco MGC in a simplex configuration. However, you can use the **prov-cpy** MML command on Cisco MGCs in high-availability or continuous-service configurations, to save and activate your changes on the active Cisco MGC. If you choose to do this, you should enter the **prov-sync** MML command immediately afterwards, to have your changes saved and activated on the standby Cisco MGC.



Note

When you enter the **prov-cpy** command, your provisioning session is also automatically ended. If you want to make additional provisioning changes, you must start a new provisioning session as described in the “Starting a Provisioning Session” section on page 3-63.



Caution

Using the **prov-sync** MML command can severely impact your system’s call processing performance. We recommend that this command be issued during a maintenance window when traffic is minimal.



Note

When the **prov-sync** MML command is used to synchronize the provisioning settings on the standby MGC host with current settings on the active MGC host, the system does not indicate when the synchronization process has failed.

The **prov-dply** MML command is used to save and activate your changes on the active and standby Cisco MGCs. This command is typically used to save and activate changes on Cisco MGCs in high-availability or continuous-service configurations. This command should not be used on a Cisco MGC in a simplex configuration.

**Note**

When you enter the **prov-dply** command, your provisioning session is also automatically ended, unless an error occurs during execution. If you want to make additional provisioning changes, you must start a new provisioning session as described in the “Starting a Provisioning Session” section on page 3-63.

Ending a Provisioning Session Without Activating your Changes

You may find that you want to end a provisioning session without saving and activating the changes you have entered during your session. If this is the case, you can enter the **prov-stp** MML command. This command ends your current provisioning session and your changes are not entered.

Invoking Dynamic Reconfiguration

You can dynamically reconfigure, that is modify or delete, select components that you have provisioned on your Cisco MGC. The following procedure lists the sequence of actions you must perform (actual steps to take depend on the provisioning tool you use):

**Note**

For more information on which components can be dynamically reconfigured, refer to the “Understanding Dynamic Reconfiguration” section on page 3-66.

- Step 1** Start a provisioning session as described in the “Starting a Provisioning Session” section on page 3-63.
- Step 2** Enter the **prov-ed** or **prov-dlt** MML commands to change or delete a component. Refer to the *Cisco Media Gateway Controller Software Release 7 Provisioning Guide* for more information on the specific structure of the command for the component type you want to dynamically reconfigure.

**Note**

To change or delete a component, you might have to meet certain preconditions, such as changing the service state of the component to *OOS* using MML commands (as mentioned in Table 3-9).

- Step 3** Repeat Step 2 for each component that you want to modify or delete. Refer to the *Cisco Media Gateway Controller Software Release 7 Provisioning Guide* for provisioning guidelines.
- Save and activate your provisioning changes as described in the “Saving and Activating your Provisioning Changes” section on page 3-64.
- Step 4** After completing a dynamic reconfiguration operation on the Cisco MGC, you must issue a service message from the associated media gateway to invoke the changes throughout your SS7 solution.

**Note**

Refer to the documentation associated with your media gateway for more information on issuing service messages.

Understanding Dynamic Reconfiguration

Dynamic reconfiguration is a function in the Cisco MGC software that allows you to modify or delete Cisco MGC components while the Cisco MGC software is still in service. Dynamic reconfiguration can be performed without shutting down or restarting either the Cisco MGC software or the Sun host platform.

The Cisco MGC component types that can be dynamically reconfigured are listed below. No other component types can be dynamically reconfigured.

- CICs
- Point codes (DPC, originating point code [OPC], or APC)
- Physical interfaces (TDM, ATM, or Ethernet)
- Signaling links (TDM, ATM, or SS7)
- Signaling services
- SS7 subsystems
- SS7 routes
- Trunk groups
- Component properties (linksets, signaling services, and trunk groups)

Table 3-1 lists the preconditions that must be met for the component before any modification or deletion action can be performed as part of dynamic reconfiguration. There are no preconditions for adding components as part of dynamic reconfiguration.

Table 3-9 Dynamic Reconfiguration Preconditions

| Component | Preconditions |
|---|--|
| CICs | <p>Call state of the CIC must be <i>IDLE</i> (refer to the “Verifying CIC States” section on page 3-13) and the service state of the associated DPC must be set to <i>OOS</i> (refer to the “Setting the Service State of a Destination” section on page 8-59).</p> <p>or</p> <p>Block type for the CIC must be set to locally blocked (refer to the “Blocking CICs” section on page 3-58) and the associated media gateway span and timeslot must be set to <i>OOS</i> (refer to the documentation for the media gateway).</p> <p>Note In Release 7.4(12), when you add CICs dynamically, you must shutdown and restore the RLM links (using the shutdown and no shutdown commands) on the associated media gateways after you provision the CICs on the Cisco MGC, to bring the CICs in to service. Refer to the documentation for your media gateway for more information on using these commands.</p> |
| Point codes (DPC, OPC, or APC) and SS7 routes | Service state of the point code and SS7 route must be set to <i>OOS</i> (refer to the “Setting the Service State of a Destination” section on page 8-59). |
| Signaling links (TDM, ATM, or SS7) | Service state of the signaling link must be set to <i>OOS</i> (refer to the “Setting the Service State of a Link or Linkset” section on page 8-60). |
| Signaling services | Service state of the signaling service must be set to <i>OOS</i> (refer to the “Setting the Service State of a Signaling Channel” section on page 8-58). |

Table 3-9 Dynamic Reconfiguration Preconditions (continued)

| Component | Preconditions |
|---|---|
| SS7 subsystems | Service state of the subsystems and routes must be set to <i>OOS</i> (refer to the “Setting the Service State of a Local Subsystem Number” section on page 8-61). |
| Trunk groups | None. |
| Component properties
(linksets, signaling services,
and trunk groups) | |

For example, if you want to change the settings for a DPC or remove it altogether, you must first set the service state of the DPC to OOS, before attempting to make changes. If you do not set the service state to OOS, your dynamic reconfiguration request is rejected with an error message.

During dynamic reconfiguration, the system goes through two phases. First, it validates the service states of all objects being changed. If any error is encountered, no reconfiguration takes place on any of the objects. Error messages indicate which components are in error. The format of the error message is “*Component’s MML name, process rejecting change, reason for rejecting the change, remedy.*”

If no errors are encountered during the validation phase, the update phase proceeds. This is where the new configuration data is loaded by all of the processes. At the beginning of the update phase, an SNMP alarm is displayed to indicate update starting. At the end of the update phase, the alarm clears, and, if commit/deploy was initiated by MML, the MML response is returned.

To change the current configuration of a component using dynamic reconfiguration, you can only use the provisioning tools provided with the Cisco MGC, MML provisioning commands or an SNMP provisioning agent (such as the Cisco MGC Manager [CMM] or the Voice Services Provisioning Tool [VSPT]).

Provisioning or configuring by using any other means can cause errors during the dynamic reconfiguration process. Using these tools is required because the dynamic reconfiguration process relies on the provisioning tools to validate the data values and, more importantly, to crosscheck the dependencies of the objects. For example, the provisioning tool ensures that adding a signal transfer point (STP) first requires the existence of the associated route.

Retrieving Provisioning Data

You can use the **prov-rtrv** MML command to retrieve information about your current provisioning settings. The ways in which you can use this command to retrieve provisioning data are described in the following sections:

- Retrieving Data for an Individual Component, page 3-68
- Retrieving Data for All Components, page 3-69
- Retrieving Data for All Components of a Particular Type, page 3-70
- Retrieving Data on the Current Provisioning Session, page 3-71
- Retrieving Data on Supported Signaling Protocols, page 3-71

Retrieving Data for an Individual Component

You can retrieve provisioning data on any individual component on your system. To do this, log in to the active Cisco MGC, start an MML session, and enter the following command:

```
prov-rtrv:component:name=MML_name
```

Where:

- *component*—The MML component type associated with the desired component. You can find a complete list of configured MML component types by performing the steps in the “Retrieving component data” section on page 3-87.
- *MML_name*—The MML name for the desired component. You can determine the MML names for the various components using the **prov-rtrv:all** MML command.

For example, to view the provisioning data for a point code called opc, you would enter the following command:

```
prov-rtrv:ptcode:name="opc"
```

The system returns a response similar to the following:

```
MGC-01 - Media Gateway Controller 2000-08-25 16:28:56
M  RTRV
    "session=active:ptcode"
    /*
    NAME = opc
    DESC = Originating Point Code
    NETADDR = 201.1.100
    NETIND = 2
    */
```

The response to the command is dependent upon the component type associated with the desired component. For example, to view the properties for an SS7 signaling service called ss7svc1, you would enter the following command:

```
prov-rtrv:sigsvccprop:name="ss7svc1"
```

The system returns a response similar to the following:

```
MGC-01 - Media Gateway Controller 2001-06-01 10:09:47
M  RTRV
    "session=active:sigsvccprop"
    /*
adjDestinations = 16
AlarmCarrier = 0
BOrigStartIndex = 0
BothwayWorking = 1
BTermStartIndex = 0
CctGrpCarrier = 2
CGBA2 = 0
CircHopCount = 0
CLIPess = 0
CotInTone = 2010
CotOutTone = 2010
CotPercentage = 0
dialogRange = 0
ExtCOT = Loop
ForwardCLIinIAM = 1
ForwardSegmentedNEED = 1
GLARE = 0
GRA2 = 0
GRSEnabled = false
```

```

InternationalPrefix = 0
layerRetries = 2
layerTimer = 10
MaxACL = 3
maxMessageLength = 250
mtp3Queue = 1024
NationalPrefix = 0
NatureOfAddrHandling = 0
Normalization = 0
OMaxDigits = 24
OMinDigits = 0
OOverlap = 0
OwnClli = na
RedirMax = 3
ReleaseMode = Async
restartTimer = 10
RoutePref = 0
sendAfterRestart = 16
slsTimer = 300
srtTimer = 300
sstTimer = 300
standard = ANSI92
SwitchID = 0
TMaxDigits = 24
TMinDigits = 0
TOverlap = 0
variant = SS7-ANSI
VOIPPrefix = 0
*/

```

Retrieving Data for All Components

You can retrieve data on all of the components provisioned on your system. To do this, log in to the active Cisco MGC, start an MML session, and enter the following command:

```
prov-rtrv:all
```

The system returns a response similar to the following:

```
MGC-01 - Media Gateway Controller 2001-06-12 17:12:49
```

```
M RTRV
```

```
"session=active:all"
```

```
/*
```

| NAME | COMPID | Parent Name | TID | Description |
|-------------------|----------|---------------|--------|--------------------|
| ----- | ----- | ----- | --- | ----- |
| "ether1" | 00050003 | "MGC-01" | CARD | "Ethernet Card 1" |
| "ether2" | 00050004 | "MGC-01" | CARD | "Ethernet Card 2" |
| "enif1" | 00060003 | "ether1" | ENETIF | "Ethernet IF 1" |
| "enif2" | 00060004 | "ether2" | ENETIF | "Ethernet IF 2" |
| "ls1" | 00080001 | "dpc1" | LNKSET | "link set 1 to |
| 2600-202-INET-6a" | | | | |
| "ls2" | 00080004 | "dpc2" | LNKSET | "link set 2 to |
| 2600-203-INET-6a" | | | | |
| "ls-itu" | 00080005 | "stp1" | LNKSET | "Lkset stp1,1-6-1" |
| "va-5300-202-1" | 00100001 | "va-5300-202" | IPLNK | "link 1 to |
| va-5300-202" | | | | |
| "va-5300-202-2" | 00100002 | "va-5300-202" | IPLNK | "link 2 to |
| va-5300-202" | | | | |
| "va-5300-203-1" | 00100003 | "va-5300-203" | IPLNK | "link 1 to |
| va-5300-203" | | | | |
| "va-5300-203-2" | 00100004 | "va-5300-203" | IPLNK | "link 2 to |
| va-5300-203" | | | | |

| | | | | |
|------------------|----------|-------------|-----------|---------------------|
| "va-5800-5-1" | 00100005 | "va-5800-5" | IPLNK | "link 1 to |
| va-5300-202" | | | | |
| "va-5800-5-2" | 00100006 | "va-5800-5" | IPLNK | "link 2 to |
| va-5800-5" | | | | |
| "route1" | 00110001 | "MGC-01" | SS7ROUTE | "route to dpc1 via |
| ls1" | | | | |
| "rt3" | 00110005 | "MGC-01" | SS7ROUTE | "SS7 Rte3-for scp2" |
| "rt1" | 00110006 | "MGC-01" | SS7ROUTE | "SS7 Rtel1-stp1" |
| "rt2" | 00110007 | "MGC-01" | SS7ROUTE | "SS7 Rte2-for scp1" |
| "route2" | 0011000a | "MGC-01" | SS7ROUTE | "route to dpc2 via |
| ls2" | | | | |
| "opc2" | 00130002 | "MGC-01" | PTCODE | "Own Pointcode" |
| "dpc2" | 00130004 | "MGC-01" | PTCODE | "TDM Switch dpc2 |
| Pointcode" | | | | |
| "opc1" | 00130006 | "MGC-01" | PTCODE | "Own Pointcode" |
| "dpc1" | 00130007 | "MGC-01" | PTCODE | "TDM Switch dpc1 |
| Pointcode" | | | | |
| "va-5300-202" | 00140001 | "nas1" | NASPATH | "Serviceto nas1" |
| "va-5300-203" | 00140002 | "nas2" | NASPATH | "Serviceto nas2" |
| "va-5800-5" | 00140003 | "nas1" | NASPATH | "Serviceto nas1" |
| "ss7svc2" | 00150002 | "dpc2" | SS7PATH | "SS7 service to |
| dpc2" | | | | |
| "ss7svc1" | 00150005 | "dpc1" | SS7PATH | "SS7 service to |
| dpc1" | | | | |
| "nas1" | 00160001 | "MGC-01" | EXTNODE | "va-5300-202" |
| "nas2" | 00160002 | "MGC-01" | EXTNODE | "va-5300-203" |
| "nas8" | 00160003 | "MGC-01" | EXTNODE | "va-5800-5" |
| "ls1link1" | 001d0001 | "ls1" | C7IPLNK | "link 1 of ls1 to |
| va-2600-202" | | | | |
| "ls2link1" | 001d0002 | "ls2" | C7IPLNK | "link 1 of ls2 to |
| va-2600-202" | | | | |
| "ls1link2" | 001d0003 | "ls1" | C7IPLNK | "link 2 of ls1 to |
| va-2600-203" | | | | |
| "ls2link2" | 001d0004 | "ls2" | C7IPLNK | "link 2 of ls2 to |
| va-2600-203" | | | | |
| "lk-3" | 001d0005 | "ls-itu" | C7IPLNK | "SS7ITU 2600-91" |
| "stp1" | 001e0001 | "MGC-01" | APC | "STP 1" |
| "scp1" | 001e0002 | "MGC-01" | APC | "SCP1 for PC/SSN" |
| "scp2" | 001e0003 | "MGC-01" | APC | "SCP2 for PC/SSN" |
| "ss7subsys3" | 001f0003 | "MGC-01" | SS7SUBSYS | "pc_ssn scp2 |
| rte-ssn 254" | | | | |
| "ss7subsys1" | 001f0004 | "MGC-01" | SS7SUBSYS | "ssn 254 (800) " |
| "ss7subsys2" | 001f0005 | "MGC-01" | SS7SUBSYS | "pc_ssn s |
| cp1 rte-ssn 254" | | | | |
| */ | | | | |

Retrieving Data for All Components of a Particular Type

You can retrieve provisioning data on all components of a particular type on your system. To do this, log in to the active Cisco MGC, start an MML session, and enter the following command:

```
prov-rtrv:component:"all"
```

Where: *component* is the MML component type associated with the desired component group. You can find a complete list of MML component types in the *Cisco Media Gateway Controller Software Release 7 Provisioning Guide*.

For example, to view the provisioning data for all point codes, you would enter the following command:

```
prov-rtrv:ptcode:"all"
```

The system returns a response similar to the following:

```
MGC-01 - Media Gateway Controller 2001-06-12 17:16:42
M   RTRV
    "session=active:ptcode"
    /*
NAME                                NETADDR      NETIND
----                                -
opc2                                2.11.1        2
dpc2                                2.2.2        2
opc1                                2.10.2        2
dpc1                                1.1.1        2
    */
```

Retrieving Data on the Current Provisioning Session

You can retrieve provisioning data on the current provisioning session. To do this, log in to the active Cisco MGC, start an MML session, and enter the following command:

```
prov-rtrv:session
```

The system returns a response similar to the following:

```
MGC-02 - Media Gateway Controller 2001-06-13 13:39:19
M   RTRV
    "session=jtest:session"
    /*
Session ID = mml1
SRCVER = active
DSTVER = jtest
    */
```

Retrieving Data on Supported Signaling Protocols

You can retrieve protocol data for the current provisioning session. To do this, log in to the active Cisco MGC, start an MML session, and enter the following command:

```
prov-rtrv:variants
```

The system returns a response similar to the following:

```
MGC-01 - Media Gateway Controller 2001-06-12 17:18:25
M   RTRV
    "session=active:variants"
    /*
MDO File name                      Protocol Family      Switch Type
-----
ANSISS7_CLEAR                      SS7-ANSI              20
ANSISS7_MCI                        SS7-ANSI              0
ANSISS7_NOATPTX                    SS7-ANSI              0
ANSISS7_SPRINT                     SS7-ANSI              0
ANSISS7_STANDARD                   SS7-ANSI              0
ATT_41459                          ISDNPRI               17
ATT_41459_C2                       ISDNPRI               17
BELL_1268                          ISDNPRI               22
BELL_1268_C3                       ISDNPRI               22
BTNUP_BTNR167                      SS7-UK                5
BTNUP_IUP                          SS7-UK                5
BTNUP_NRC                          SS7-UK                5
DPNSS_BTNR188                      DPNSS                 26
EISUP                              EISUP                 0
ETS_300_102                        ISDNPRI               27
ETS_300_102_C1                     ISDNPRI               27
    */
```

| | | | |
|---------------------------|-----------|----|----|
| ETS_300_102_C6 | ISDNPRI | 27 | |
| ETS_300_121 | SS7-ITU | 0 | |
| ETS_300_172 | ISDNPRI | 29 | |
| ETS_300_356 | SS7-ITU | 0 | |
| HKTA_2202 | SS7-ITU | 0 | |
| ISUPV1_POLI | SS7-ITU | 0 | |
| ISUPV2_32DIG | SS7-ITU | 0 | |
| ISUPV2_CZECH | SS7-ITU | 0 | |
| ISUPV2_FINNISH96 | SS7-ITU | 0 | |
| ISUPV2_FRENCH | SS7-ITU | 0 | |
| ISUPV2_GERMAN | SS7-ITU | 0 | |
| ISUPV2_JAPAN | SS7-Japan | 10 | |
| ISUPV2_KPNPB | SS7-ITU | 0 | |
| ISUPV2_NTT | SS7-Japan | 0 | |
| ISUPV2_SPANISH | SS7-ITU | 0 | |
| ISUPV2_SWISS | SS7-ITU | 0 | |
| ISUPV2_TELEFONICA | SS7-ITU | 0 | |
| ISUPV2_VIETNAM | SS7-ITU | 0 | |
| ISUPV3_UK | SS7-UK | 0 | |
| ISUPV3_UK_AXE10 | SS7-UK | 15 | |
| ISUPV3_UK_AXE10_BTNETCHAT | SS7-UK | | 15 |
| ISUPV3_UK_BTNETCHAT | SS7-UK | 0 | |
| Q721_BASE | SS7-ITU | 5 | |
| Q721_BRAZILIAN | SS7-ITU | 5 | |
| Q721_CHINA | SS7-China | 5 | |
| Q721_FRENCH | SS7-ITU | 5 | |
| Q721_PHILLIPINE | SS7-ITU | 5 | |
| Q761_ARGENTINA | SS7-ITU | 0 | |
| Q761_ARGENTINA_C2 | SS7-ITU | 0 | |
| Q761_AUSTRAL | SS7-ITU | 0 | |
| Q761_AUSTRAL_C2 | SS7-ITU | 0 | |
| Q761_BASE | SS7-ITU | 0 | |
| Q761_BELG_BCOM | SS7-ITU | 0 | |
| Q761_BELG_ISUP_CUJO | SS7-ITU | 0 | |
| Q761_BELG_MOBI | SS7-ITU | 0 | |
| Q761_CHILE | SS7-ITU | 0 | |
| Q761_CHINA | SS7-China | 0 | |
| Q761_CHINA_MOB | SS7-China | 0 | |
| Q761_CHINA_MOB | SS7-ITU | 0 | |
| Q761_DANISH | SS7-ITU | 0 | |
| Q761_INDIA | SS7-ITU | 0 | |
| Q761_KOREAN | SS7-ITU | 0 | |
| Q761_NEWZEALAND | SS7-ITU | 0 | |
| Q761_PERU | SS7-ITU | 0 | |
| Q761_PORTUGAL | SS7-ITU | 0 | |
| Q761_SIEMENS_MOBI | SS7-ITU | 0 | |
| Q761_SINGAPORE | SS7-ITU | 0 | |
| Q761_TAIWAN | SS7-ITU | 0 | |
| Q761_THAILAND | SS7-ITU | 0 | |
| Q767_BASE | SS7-ITU | 0 | |
| Q767_BRAZIL | SS7-ITU | 0 | |
| Q767_COLOMBIA | SS7-ITU | 0 | |
| Q767_GUATEMALA | SS7-ITU | 0 | |
| Q767_INDONESIA | SS7-ITU | 0 | |
| Q767_ITAL | SS7-ITU | 0 | |
| Q767_ITAL_INTERCONNECT | SS7-ITU | | 0 |
| Q767_MEXICAN | SS7-ITU | 0 | |
| Q767_RUSS | SS7-ITU | 0 | |
| Q767_SPAN | SS7-ITU | 0 | |
| Q767_SWED | SS7-ITU | 0 | |
| Q767_TELSTRA | SS7-ITU | 0 | |
| Q767_TURKISH | SS7-ITU | 0 | |
| T113_BELL | SS7-ANSI | 0 | |
| dummy | AVM | 0 | |


```

dummy          MGCP          0
dummy          SGCP          0
dummy          TCAPOverIP    0
dummy          VSI           0
*/

```

Provisioning a Dial Plan

You can provision dial plans on your Cisco MGC using the commands listed below. For more information on provisioning and maintaining dial plans, refer to the *Cisco Media Gateway Controller Software Release 7 Dial Plan Guide*.

- **chg-dpl**—Reloads dial plans based on customer group ID number.
- **numan-add**—Adds an element to a dial plan.
- **numan-dlt**—Deletes an element from a dial plan.
- **numan-ed**—Edits an existing element in a dial plan.
- **numan-rtrv**—Displays information pertaining to an element or all elements in a dial plan.



Note

You can verify dial plans using the translation verification viewer on the Cisco MGC toolbar. For information on using the translation verification viewer, refer to the “Verifying a Dial Plan Translation” section on page 3-118.

Importing Provisioning Data

You can import provisioning data files (created using the **prov-exp** MML command) and execute the MML commands contained in those files in batch mode to copy the set up from another system, or return a system to a baseline configuration. Refer to the “Exporting Provisioning Data” section on page 3-74 for more information on exporting provisioning data.

To import the provisioning data files and execute the MML commands in batch mode, log in to the active Cisco MGC, and enter the following UNIX command:

```
mml -b export_directory_path/filename
```

Where:

- *export_directory_path*—The directory path to the location of the exported provisioning data files.
- *filename*—The name of the provisioning data file you want to import.

The provisioning data files must be provisioned in the following order:

- *config.mml*—Contains core configuration data (signaling services, SS7 nodes)
- *export_trunks.dat* (created only when trunks are configured on your system)
- *export_trkgrp.dat* (created only when trunk groups are configured on your system)
- *routing.mml*—Contains routing plans
- *custGrpID.mml*—One of these files is created for each existing dial plan, with the file being named with the associated customer group ID number.

For example, to import the provisioning data stored in the *config.mml* file, which is located in the */opt/CiscoMGC/etc/cust_specific/saved_config* directory, you would enter the following command:

```
mml -b /opt/CiscoMGC/etc/cust_specific/saved_config/config.mml
```

Exporting Provisioning Data

You can use the **prov-exp** MML command to export the current provisioning set up of your Cisco MGC in MML-command form to a file or files. This allows you to copy the provisioning data from one Cisco MGC and set up another Cisco MGC with that same provisioning data or to restore a Cisco MGC to a baseline provisioning environment. Refer to “Importing Provisioning Data” section on page 3-73 for information on importing the provisioning data created by the **prov-exp** MML command.

To export part of the current configuration of your Cisco MGC to a file, log in to the active Cisco MGC, start an MML session, and enter the following command:

```
prov-exp:tid:dirname="export_directory_name"
```

Where:

- *tid*—Types of data. These can be:
 - *config*—Core configuration data (signaling services, SS7 nodes), including trunks and trunk groups. This selection creates the following files: *config.mml*, *export_trunks.dat* (created only when trunks are configured on your system), and *export_trkgrp.dat* (created only when trunk groups are configured on your system).
 - *routing*—Routing plans. This selection creates a file called *routing.mml*
 - *numan*—Dial plans. This selection creates a file for each dial plan specified on your system. The file name is dependent on the customer group ID for each dial plan, that is the names of the files follows the format *custGrpID.mml*.
- *export_directory_name*—Name of the directory to which the data is exported. This directory is a subdirectory within the */opt/CiscoMGC/etc/cust_specific* directory established at installation.

For example, to export the core configuration data to a file stored in the */opt/CiscoMGC/etc/cust_specific/saved_config* directory, you would enter the following command:

```
prov-exp:config:dirname="saved_config"
```

To export all of the current configuration of your Cisco MGC to several files, log in to the active Cisco MGC, start an MML session, and enter the following command:

```
prov-exp:all:dirname="export_directory_name"
```

Where *export_directory_name* is the name of the directory to which the data is exported. This directory is a subdirectory within the */opt/CiscoMGC/etc/cust_specific* directory established at installation.

The system creates the following files in the specified directory when this command is entered:

- *config.mml*—Contains core configuration data (signaling services, SS7 nodes)
- *export_trunks.dat* (created only when trunks are configured on your system)
- *export_trkgrp.dat* (created only when trunk groups are configured on your system)
- *routing.mml*—Contains routing plans
- *custGrpID.mml*—One of these files is created for each existing dial plan, with the file being named with the associated customer group ID number.

For example, to export all of the provisioning data into files stored in the */opt/CiscoMGC/etc/cust_specific/saved_config* directory, you would enter the following command:

```
prov-exp:all:dirname="saved_config"
```

Managing Automatic Congestion Control

The Cisco MGC supports Automatic Congestion Control (ACC). ACC dynamically regulates incoming traffic on the Cisco MGC to levels that can be handled effectively by rejecting a percentage of new calls when the Cisco MGC is congested. ACC increases the throughput of completed calls through the telephone network during periods of overload.

During periods of overload on the Cisco MGC, a user-defined percentage (depending on internal congestion level) of incoming calls are rejected and an ISUP release message is sent to the adjacent signaling point. That ISUP release message has a clear cause of Switch Equipment Congestion and contains an Automatic Congestion Level (ACL) value that indicates the overload level of the Cisco MGC. For a call that is in progress when overload occurs and the call clears normally, the ISUP release message has a clear cause of Normal Call Clearing and an ACL value associated with the current overload level of the Cisco MGC.

ACC is controlled by parameters that are found in the XECfgParm.dat file and by a property associated with the signaling service or trunk group, which are described in the following sections:

- Understanding Overload Level Percentage Parameters, page 3-75
- Understanding the CPU Timer Interval Parameter, page 3-78
- Understanding the Maximum ACL Value, page 3-78
- Modifying the Maximum ACL Value, page 3-79
- Retrieving Overload Level, page 3-80

Understanding Overload Level Percentage Parameters

The overload level (or congestion level) of the Cisco MGC is measured in three levels (1, 2, and 3, with 3 being the highest). Each overload level has three associated thresholds, one for overload onset, one for overload abatement, and one more for the percentage of calls that are rejected during an overload condition. These thresholds are defined by parameters found in the XECfgParm.dat file.

The XECfgParm.dat parameters that are used to set the overload level thresholds are listed below.

- Ovl1OnsetThresh—Percentage of total CPU utilization at which overload level 1 is reached. The default value is 82. The range of valid values is 0 through 100.
- Ovl1AbateThresh—Percentage of total CPU utilization at which overload level 1 abates. The default value is 75. The range of valid values is 0 through 100.
- Ovl1RejectPercent—Percentage of calls that are rejected while overload level 1 is active. The default value is 25. The range of valid values is 0 through 100.
- Ovl2OnsetThresh—Percentage of total CPU utilization at which overload level 2 is reached. The default value is 90. The range of valid values is 0 through 100.
- Ovl2AbateThresh—Percentage of total CPU utilization at which overload level 2 abates. The default value is 77. The range of valid values is 0 through 100.
- Ovl2RejectPercent—Percentage of calls that are rejected while overload level 2 is active. The default value is 50. The range of valid values is 0 through 100.
- Ovl3OnsetThresh—Percentage of total CPU utilization at which overload level 3 is reached. The default value is 93. The range of valid values is 0 through 100.
- Ovl3AbateThresh—Percentage of total CPU utilization at which overload level 3 abates. The default value is 85. The range of valid values is 0 through 100.
- Ovl3RejectPercent—Percentage of calls that are rejected while overload level 3 is active. The default value is 100. The range of valid values is 0 through 100.

You can configure the onset, abatement, and rejection thresholds for CPU utilization using these XECfgparm.dat parameters. The default values for these parameters enable the Cisco MGC to operate in conformance with Q.543, section 3. You can modify these values experimentally, based on your network's traffic patterns, to enhance the performance of your Cisco MGC.

**Note**

The instructions for modifying the XECfgParm.dat file are found in the *Cisco Media Gateway Controller Software Release 7 Installation and Configuration Guide*.

**Caution**

Changing the ACC-related parameters in the XECfgParm.dat file requires that the Cisco MGC software be shut down and then re-started. If you decide to modify the parameters in the XECfgParm.dat file, you must contact the Cisco TAC before shutting down the Cisco MGC software.

The overload level is tracked using three measurements, which are described in Table 3-10.

Table 3-10 Overload Level Measurement Types

| Measurement | Frequency | Calculation |
|--|---|--|
| Mean CPU utilization level | Per CPU utilization interval (user-defined) | Mean of the average CPU utilization levels over the duration of the CPU utilization interval is compared to the overload level thresholds. |
| Engine thread utilization level | Per CPU utilization interval (user-defined) | Utilization level for the engine thread with the highest average usage level over the duration of the CPU utilization interval is compared to the overload level thresholds. There are three engine threads: <ul style="list-style-type: none"> • CallProc1 • CallProc2 • Dispatcher Note The number of engine threads is equal to the XECfgParm.dat file parameter, *.numOfThreads, plus 1 ($(*.numOfThreads = 2) + 1 = 3$). |
| Call processing engine queue occupancy level | Per new call | Current size of queue is divided by the capacity of the queue and compared to the queue occupancy overload thresholds. The queue occupancy overload thresholds are equal to half of the value of the corresponding overload level thresholds.

Note The queue occupancy thresholds are half the value of the overload level thresholds due to the high sensitivity of the measurement. For more information on the CPU utilization interval XECfgParm.dat parameter, refer to the “Understanding the CPU Timer Interval Parameter” section on page 3-78 |

Overload conditions are most likely to be caused by high CPU utilization levels, since the Cisco MGC software uses multi-threaded processing, which almost eliminates the possibility that the size of the call processing engine queue would exceed the queue occupancy overload thresholds. For information on viewing the current overload level, refer to the “Retrieving Overload Level” section on page 3-80.

When any of the three overload measurement types indicate that an overload onset threshold has been passed, the Cisco MGC generates an alarm associated based on the overload level. Table 3-11 details the overload level to alarm relationship. For more information on these alarms, refer to the *Cisco Media Gateway Controller Software Release 7 Messages Reference Guide*.

Table 3-11 Alarm Associations for Cisco MGC Overload Levels

| Cisco MGC Overload Level | Associated Alarm |
|--------------------------|------------------|
| 1 | OverloadLight |
| 2 | OverloadMedium |
| 3 | OverloadHeavy |

The alarms are automatically cleared when the associated overload measurement is re-taken and a new overload level has been reached, either dropping to the associated abatement threshold or rising to a higher onset threshold. For example, if, over three consecutive CPU utilization interval timer periods, the CPU utilization level measurement indicated that the overload level is 3 for the first period, that the overload level is 1 for the second period, and that the overload level is 2 for the third period, the system would go through the following process:

1. CPU utilization interval timer expires, Cisco MGC has an overload level of 3.
2. OverloadHeavy alarm is set.
3. CPU utilization interval timer expires, Cisco MGC has an overload level of 1.
4. The OverloadHeavy alarm is cleared.
5. The OverloadLight alarm is set.
6. CPU utilization interval timer expires, Cisco MGC has an overload level of 2.
7. The OverloadLight alarm is cleared.
8. The OverloadMedium alarm is set.



Note

It is possible that during the time period for the above example, several overload level alarms associated with an overloaded call processing engine queue could also be set and cleared. Overload level for the call processing queue is determined for each incoming call to protect the system against short-term spikes in the call arrival rate.



Note

The alarms associated with the Cisco MGC's overload level create SNMP traps. To identify these alarms among the SNMP traps, look for the tpAlarmCatName object to contain the name of the alarm (OverloadLight, OverloadMedium, or OverloadHeavy) and the tpAlarmSet object to indicate whether the alarm is being set (2) or cleared (1). For more information on the MIBs for the Cisco MGC, refer to the *Cisco Media Gateway Controller Software Release 7 Management Information Base Guide*.

Understanding the CPU Timer Interval Parameter

The XECfgParm.dat parameter, CPUTimerInterval, is used to specify the interval, in milliseconds, at which the average CPU utilization level of the Cisco MGC is sampled. The default value is 3000. We recommend that you stay within the range of 1000 to 4000 milliseconds. A lower interval rate provides a quicker response to internal congestion, while a higher interval rate provides a more accurate sample.

**Note**

The overload level jumps from one level to another, depending entirely on the value of each overload measurement at the time of the sample. The overload level does not step through each level to change from lower-levels to higher-levels or vice-versa.

**Note**

The instructions for modifying the XECfgParm.dat file are found in the *Cisco Media Gateway Controller Software Release 7 Installation and Configuration Guide*.

**Caution**

Changing the ACC-related parameters in the XECfgParm.dat file requires that the Cisco MGC software be shut down and then re-started. If you decide to modify the parameters in the XECfgParm.dat file, you must contact the Cisco TAC before shutting down the Cisco MGC software.

Understanding the Maximum ACL Value

When the Cisco MGC is overloaded, an ACL value is sent to adjacent signaling points in an ISUP release message. 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 ACC maximum overload level value to the maximum ACL value used by the adjacent signaling point.

ANSI-based signaling points have a maximum ACL value of 3, ITU-based signaling points have a maximum ACL value of 2, and the ACC maximum overload level value is 3. When MaxACL is set to 3, the ACC maximum overload value is mapped to the ANSI standard, (the default value for MaxACL is 3). When MaxACL is set to 2, the ACC maximum overload value is mapped to the ITU standard. MaxACL also has a third possible setting, 0, which disables the sending of ACL indications in the ISUP release message. Table 3-12 shows how the MaxACL settings map the ACC maximum overload value to the ANSI and ITU congestion standards.

**Note**

Disabling the MaxACL parameter (setting it to '0') does not disable the ACC functionality. If the MaxACL parameter is set to '0' and the Cisco MGC becomes congested, the percentage of calls specified for that overload level are released, and the associated ISUP release message does not contain an ACL indication. The ISUP release message still indicates the proper clear cause.

Modifying the Maximum ACL Value

To modify the maximum ACL value using MML commands, perform the following steps:



Note

You can use the CMM or the VSPT to modify the maximum ACL value on your system. Refer to the *Cisco Media Gateway Controller Software Release 7 Provisioning Guide* for more information about using the CMM or VSPT to modify the properties of an SS7 signaling service or a trunk group.

Step 1 Start a provisioning session, as described in the “Starting a Provisioning Session” section on page 3-63.

Step 2 Enter the following command to set the property that maps the internal maximum ACL value to the value expected by the adjacent signaling point:

```
prov-ed:component:name="comp_name",MaxACL=num
```

Where:

- *component*—MML component type name for the SS7 signaling service or trunk group properties. Enter one of the following:
 - *ss7path*—Component type for SS7 signaling services.
 - *trnkgrp*—Component type for trunk groups.
- *comp_name*—MML name for the SS7 signaling service or trunk group on which you are mapping the internal maximum ACL value to the value expected by the adjacent signaling point.
- *num*—Number that indicates how to map the maximum ACL values. Table 3-12 lists the valid values for this parameter and their associated congestion levels.

Table 3-12 Maximum ACL Mapping Values

| MaxACL Value | Associated Congestion Standard | Cisco MGC ACC Overload Levels | Corresponding ACL Values |
|--------------|--------------------------------|-------------------------------|-----------------------------------|
| 0 | N/A | N/A | Disables the creation of ACL |
| 2 | ITU | N/A
1
2
3 | 0 (No ACL present)
1
2
2 |
| 3 | ANSI | N/A
1
2
3 | 0 (No ACL present)
1
2
3 |

For example, to modify the internal maximum ACL value on a trunk group named **trunk1**, which is adjacent to a signaling point that uses the ITU congestion standard, you would enter the following command:

```
prov-ed:trnkgrp:name="trunk1",MaxACL=2
```

For example, to modify the internal maximum ACL value on an SS7 signaling service named **ss7svc1**, which is adjacent to a signaling point that uses the ITU congestion standard, you would enter the following command:

```
prov-ed:ss7path:name="ss7svc1",MaxACL=2
```

- Step 3** Save and activate your provisioning changes as described in the “Saving and Activating your Provisioning Changes” section on page 3-64.
-

Retrieving Overload Level

To retrieve the current overload level of your system, log in to the active Cisco MGC, start an MML session, and enter the following command:

```
rtrv-ovld
```

The system returns a response that identifies the current overload level (0 through 3) and number of messages in the call engine queue.

```
Media Gateway Controller - MGC-01 2000-01-12 15:19:51
M RTRV
"ENGG-01: OVLD=0,MSGQ=0"
```

Managing your Cisco MGC Platform

The operations you can use to manage your Cisco MGC platform are described in the following sections:

- Performing a Manual Switchover, page 3-80
- Verifying Successful Completion of a Switchover, page 3-82
- Verifying the Patch Level of the Cisco MGC, page 3-85
- Retrieving Configuration Table Data, page 3-87
- Retrieving the Logging Level of Software Processes, page 3-89

Performing a Manual Switchover

In the continuous service configuration, you can swap the roles of the active Cisco MGC and the standby Cisco MGC by invoking the appropriate MML command from the management interface of the active Cisco MGC. A switchover can be done only from the active Cisco MGC, because only the active Cisco MGC can command the standby Cisco MGC to take over. If there is only one Cisco MGC processing all calls, a manual switchover request is rejected.

Manual switchovers are typically performed for the following reasons:

- To periodically switch the roles of the Cisco MGCs
- To upgrade the existing software to a new release
- To bring down a system for hardware maintenance

When you need to order a manual switchover to perform maintenance or upgrade procedures on one or both of the Cisco MGCs, use the following steps or all calls might be killed by the call engine. Starting with both the active and standby Cisco MGCs operating normally, you can invoke a manual switchover from one system to the other by completing the following steps:

-
- Step 1** Determine whether both the active and standby Cisco MGCs are operating normally, as described in the “Verifying the Platform State of the Cisco MGC Hosts” section on page 3-2.
- Step 2** Determine whether any alarms are pending on either system, as described in the “Monitoring the Alarms Status” section on page 3-6.

If any alarms are pending, you must correct the situation that caused the alarms. Search for the corrective actions required to clear any alarms in the “Alarm Troubleshooting Procedures” section on page 8-8. If the alarms do not appear in that section, corrective action is not required for those alarms. Refer to the *Cisco Media Gateway Controller Software Release 7 Messages Reference Guide* for more information on those alarms.

Step 3 Ensure that calls are being replicated from the active Cisco MGC to the standby Cisco MGC, as described in the “Verifying Proper Replication of Calls” section on page 3-56.

Step 4 Enter the following MML command to synchronize the provisioning data on the standby Cisco MGC with the data on the active Cisco MGC:

```
prov-sync
```

**Caution**

Using the **prov-sync** MML command can severely impact your system’s call processing performance. We recommend that this command be issued during a maintenance window when traffic is minimal.

Step 5 Determine platform state of both Cisco MGCs, as described in the “Verifying the Platform State of the Cisco MGC Hosts” section on page 3-2.

Step 6 Check that all the processes on the active Cisco MGC are in the running state, as described in the “Verifying That Processes Are Running” section on page 3-3.

**Caution**

The next step forces a manual switchover to the standby Cisco MGC. Ensure that the standby Cisco MGC is fully operational and that debugging is turned off before taking the active Cisco MGC OOS, or there might be a total interruption of service.

Switchover can also cause call processing to fail if debugging is turned on.

**Caution**

If you are using a software version prior to Release 7.4(11), we recommend that you limit the number of configuration versions stored in the configuration library to 64. We recommend this limitation because during a switchover operation or use of the **prov-sync** command, the standby MGC attempts to synchronize all of its system configurations with those stored in the active Cisco MGC. If you are storing a more than 64 system configurations, the state transition can fail and the standby Cisco MGC goes to an OOS state. For more information about administering the configuration library, refer to the “Using the Config-Lib Viewer” section on page 3-113. If you are using software release 7.4(11) or higher, the disk monitor script automatically controls the number of versions stored in the configuration library. Refer to the *Release Notes for the Cisco Media Gateway Controller* for more information. For more information about the disk monitor script, refer to the “Automatic Disk Space Monitoring” section on page 3-24.

Step 7 Log in to the active Cisco MGC, start an MML session, and enter the following command:

```
sw-over::confirm
```

Site alarms are automatically set until the OOS Cisco MGC is returned to an IS state.

Step 8 Verify that the switchover has been successfully performed. To do this, follow the procedure described in the “Verifying Successful Completion of a Switchover” section on page 3-82.

Verifying Successful Completion of a Switchover

You can determine whether a switchover (automatic or manual) was successfully completed by retrieving the status of each Cisco MGC. Once all of the processes to come up (the time it takes for this to happen depends on the amount of traffic), determine the platform state of both Cisco MGCs, as described in the “Verifying the Platform State of the Cisco MGC Hosts” section on page 3-2. If the platform state of both Cisco MGCs was as expected, the switchover was successfully completed. If one of the Cisco MGCs does not return the expected platform state, the switchover was not successfully completed. Refer to the “Recovering from a Switchover Failure” section on page 8-113.

Understanding Switchover

Cisco MGCs can be arranged in an Active-Standby configuration in which one MGC host runs active traffic while checkpointing information to the standby Cisco MGC. In the continuous service configuration, the active Cisco MGC is paired with an identical standby Cisco MGC that automatically takes over if a failure or switchover occurs. The continuous service architecture of the Cisco MGC increases the reliability, availability, and failure-aversion capabilities of the system.

The primary goal of the Cisco MGC failover subsystem is to ensure call preservation when there is a system failure. This is achieved by interconnecting two Cisco MGCs while the system carries out the logical functions of call control. At any point, one Cisco MGC is in the active role and the other Cisco MGC is in the standby role. The active Cisco MGC carries out the call control function and updates the standby Cisco MGC about call-processing events. The standby Cisco MGC maintains the same system state (from the call-processing point of view) as the active Cisco MGC. In the event of a critical failure on the active Cisco MGC, the standby switches to the active role and takes over the call control function, ensuring that all established calls are preserved.

**Note**

If your system is using a simplex configuration (a single Cisco MGC), or is functioning in standalone mode (the standby Cisco MGC is in the OOS service state), the system cannot perform a switchover. In these instances, the active Cisco MGC remains in the active service state when a critical failure occurs.

Switchovers can occur automatically (also known as failovers) when a critical alarm is generated, or a switchover can be performed manually, typically as part of a maintenance or troubleshooting procedure. For more information on performing a manual switchover, refer to the “Performing a Manual Switchover” section on page 3-80.

**Note**

When a failover is caused by the temporary loss of all Cisco MGC/IP continuity, the newly standby Cisco MGC can take upwards of 6 minutes to come in-service.

Fault-Tolerant Components

The following component processes of the Cisco MGC are fault-tolerant. In other words, each of these processes knows its own state (Active/Standby/Out-of-Service) and the corresponding state of its peer process on the standby system.

- Process manager (procM)—Spawns and manages all processes in the system
- Failover daemon (foverd)—Determines and switches platform states
- Call engine—Handles call-processing functions
- Replicator—Replicates call states from the active Cisco MGC to the standby Cisco MGC
- I/O channel controller (IOCC)—Manages the signaling messages

- I/O channel manager (IOCM)—Manages the protocol-specific IOCCs

Failover Daemon

The active Cisco MGC runs the procM process. ProcM automatically starts when the Cisco MGC is booted and, in turn, starts the alarm manager, configuration manager, call engine, IOCCs, and other processes, including foverd.

The continuous service architecture is controlled by the failover daemon. The failover daemons on both Cisco MGC hosts coordinate the active, standby, and OOS states of those hosts.

The alarm manager process also plays a significant role in a continuous service system. The alarm manager raises the alarm when a critical event occurs and clears the alarm when the condition that caused the alarm is cleared. See the *Cisco Media Gateway Controller Software Release 7 Messages Reference Guide* for detailed information regarding alarms, specifically which alarms are critical.

The foverd process directs manual switchovers. The switchover configuration provides the following:

- Minimal interruption of service in the event of failure of a single machine
- Maintenance of a consistent configuration on both the active and standby Cisco MGCs
- Avoidance of false switchovers that could cause disruption of service

A critical event is typically a critical process dying or the failure of a subsystem or component that can critically affect call processing. A forced failover occurs automatically when the conditions governing it are met; it is system-initiated and not user-initiated. When a critical event occurs, the alarm manager sends a specific message to the foverd process, indicating the occurrence of the critical event.

When the failover daemon receives notification that a critical event has occurred on the active Cisco MGC, the failover daemon initiates a forced switchover to the standby Cisco MGC. The standby Cisco MGC transitions immediately to the active state; established calls are maintained, but calls still in the process of being set up are lost.

The occurrence of a critical event on system A results in its peer, system B, becoming active while system A goes to an OOS state. Until the critical event that triggered the failover on system A is cleared, its state remains OOS. When the critical event is cleared, the alarm manager sends another message, known as a Clear Alarm message, to the foverd process. The foverd process drives system A to a standby state (if the peer system (B) is still in the active state).

When the critical event is cleared, the failed controller (A) comes back online. It can then become the standby for the currently active Cisco MGC (B). Initially, system A is still OOS. The platform state of system A continues to be OOS until the critical event is cleared.

Established calls are maintained during a switchover because the Call Engine checkpoints call information from the active Cisco MGC to the standby Cisco MGC. In addition, the state of the SS7 network is checkpointed by the MTP3 IOCC. The MTP2 terminal functionality resides on the Cisco SLTs to enable the fault-tolerant MTP3 solution.

The Cisco SLTs are responsible for SS7 MTP2 message processing. The Cisco SLTs communicate directly with the Cisco MGC hosts (active and standby) using RUDP, but they send SS7 traffic only to the active Cisco MGC.



Note

The number of Cisco SLTs is dependent on the SS7 network traffic load and on link and linkset requirements. It is generally recommended that a minimum of two links per linkset, one link per Cisco SLT, be used to provide SS7 reliability. To further enhance redundancy, it is recommended that the links in a linkset be spread across multiple Cisco SLTs so that any single unit can be removed, added, or serviced without disrupting the SS7 network.

Circuit Auditing

An auditing process discovers discrepancies in circuit states between the Cisco MGC and the media gateways it controls. During a switchover, discrepancies might exist as to the state of bearer circuits (CICs) between the newly active Cisco MGC and the bearer devices it controls. Discrepancies in circuit states between the active Cisco MGC and the bearer devices could also occur as the result of control messages to the bearer devices that get lost.

The circuit auditing mechanism can be run periodically at configured intervals or after an automatic or manual switchover. It can also be initiated manually using the MML command, **sw-over::confirm**. The audit capability is always initiated automatically on indication of critical error conditions from solution components, adjacent SS7 switches, or when critical Cisco MGC conditions occur. The circuit-auditing mechanism detects and resolves circuit state discrepancies that it discovers and resynchronizes the Cisco MGC and the bearer devices.



Caution

If you are using software prior to release 7.4(11), we recommend that you limit the number of configuration versions stored in the configuration library to 64. We recommend this limitation because during a switchover operation or use of the **prov-sync** command, the standby MGC attempts to synchronize all of its system configurations with those stored in the active Cisco MGC. If you are storing a more than 64 system configurations, the state transition can fail and the standby Cisco MGC goes to an OOS state. For more information about administering the configuration library, refer to the “Using the Config-Lib Viewer” section on page 3-113. If you are using software release 7.4(11) or higher, the disk monitor script automatically controls the number of versions stored in the configuration library. Refer to the *Release Notes for the Cisco Media Gateway Controller Software* for more information. For more information about the disk monitor script, refer to the “Automatic Disk Space Monitoring” section on page 3-24.

The circuit auditing mechanism is a function of the call engine process in the active Cisco MGC. The call engine subsystem starts a thread to perform the circuit-auditing function upon notification of a switchover event from the fault manager.

The circuit auditing mechanism commands the bearer devices to reflect the circuit state of the Cisco MGC. If a bearer device believes the circuit to be in use and the Cisco MGC does not, the Cisco MGC releases the circuit. However, if the Cisco MGC shows that a bearer circuit is in use and discovers that the bearer device does not show that circuit as in use, the Cisco MGC does not attempt to rebuild the call, but releases all associated resources. Even though the Cisco MGC is the controlling authority, the only course of action when a discrepancy is discovered during a circuit audit is to release all of the allocated resources, which means dropping the call.

Checkpointing

Checkpointing of calls ensures that established calls are preserved in the event of a switchover. The Call Engine sends checkpoint events to the local checkpoint process at one point during call setup and at one point in the call release phase.

Checkpointing is also applied to the following protocol supervisory messages and MML commands that change the logical state of the bearer circuits:

- Blocking and Unblocking Messages and Commands
- Circuit Reset Messages and Commands

The local checkpointing process is responsible for securing these events to disk if the standby Cisco MGC is unavailable and for forwarding those events to the remote checkpointing process once it does become available. If the standby Cisco MGC is running, checkpoint events are batched and forwarded to the remote checkpointing process.

The remote checkpointing process is responsible for handling the checkpoint events from the active Cisco MGC, delivering only established calls to the remote call engine. The remote call engine process begins checkpointing events for calls when it begins active call processing.

The following scenarios are supported:

- Standalone (no standby Cisco MGC available)—You can specify the activation or deactivation of checkpointing. If checkpointing is activated, all checkpoint events are secured to disk.
- Startup (standby Cisco MGC unavailable)—The local checkpointing process retains or secures all events until the standby Cisco MGC is available and a request for synchronization is completed.
- Synchronization—You can request synchronization of the configurations of the two Cisco MGCs. This is required after startup and transition from the standalone Cisco MGC to the standby available configuration.
- Switchover—In the event of a switchover (or failover), the standby Cisco MGC assumes the primary responsibility for processing calls and securing checkpoint events.

Checkpointing is also implemented to support forward Cisco MGC software migration by one release. You can manually take the standby Cisco MGC out of service, upgrade the software to the new release, and resynchronize calls with the active Cisco MGC. For detailed procedures on upgrading the Cisco MGC software, refer to the *Cisco Media Gateway Controller Software Release 7 Installation and Configuration Guide*.

Verifying the Patch Level of the Cisco MGC

As of Release 7.4(12) of the Cisco MGC software, you can verify the patch level of your Cisco MGC software by performing the following steps:

- Step 1** Display the current patch level of your system by logging into the active Cisco MGC as root and entering the following UNIX command:

```
pkginfo | grep Patch
```

The system returns a response similar to the following:

| | | |
|-------------|-----------|---|
| application | CSCOgp003 | Cisco Media Gateway Controller Software Patch Package |
| application | CSCOgp009 | Cisco Media Gateway Controller Software Patch Package |
| application | CSCOgs003 | Cisco Media Gateway Controller Software Patch Package |
| system | SUNWswmt | Patch Utilities |

Look for the Cisco MGC patch with the largest number to determine the current patch level. In the example, the current protocol patch level is patch 9 (CSCOgp009), while the system patch level is patch 3 (CSCOgs003).



Note For more information on the patches to the release of the Cisco MGC software you are running, refer to the release notes associated with your release. To determine which release of the Cisco MGC software you are running, enter the **rtv-ne** MML command, as described in the “Verifying the Platform State of the Cisco MGC Hosts” section on page 3-2.

- Step 2** Determine the patches available for your version of Cisco MGC software by entering the following URL on an Internet browser:

<http://www.cisco.com/kobayashi/sw-center/sw-voice.shtml>

Select your software version from the list and a list of currently available patches displays.

If you find that your patch level matches the current patch level on the web page, the procedure is complete. Otherwise, proceed to Step 3.

Step 3 Download the latest patches and associated installation instruction files to your active Cisco MGC.

Step 4 Open the instruction files and follow the procedures within to install the patches.

Step 5 Once you have installed the new patches, run the check inventory utility to ensure that the patches have installed correctly by entering the following UNIX commands:

**Caution**

This utility should not be run while the system is actively processing calls, as it can reduce the call processing rate.

**Note**

This utility can only be run by a user with root permissions. If you are not logged in as root, you must enter the UNIX command **sudo** before the utility name to ensure proper execution.

```
cd /opt/CiscoMGC/bin
chk_inv [>file_path]
```

**Note**

You must be in the /opt/CiscoMGC/bin directory to run the check inventory utility.

Where *file_path* is an optional parameter used when you want to redirect the output of the utility to a file. If you do not redirect the output to a file, the results are written to your screen.

For example, to redirect the results of the check inventory utility to a file called inv.out, you would enter the following command:

```
chk_inv >/opt/CiscoMGC/local/inv.out
```

Step 6 Review the utility results, either on-screen or by opening the file. If the results indicate that there are no problems with the installation, the procedure is complete. Otherwise, proceed to Step 7.

**Caution**

The check inventory utility uses a 32-bit cyclic redundancy check (CRC) to verify your system's software. A 32-bit CRC can have a value anywhere from 1 to over 4 billion. However, there is a slight possibility that two sets of data can have the same CRC value. If this should occur, you will receive a false positive from the utility.

**Note**

If the utility results indicate that there is a problem with a part of the software outside of the Cisco MGC software patch(es), you should determine whether a problem truly exists. The utility compares the software on your system against a master list, and it is possible that your environment may not be using every piece of software on that master list. If the utility indicates that a piece of software is missing, and your system configuration does not use that software, you do not need to load that software. However, if the utility identifies a problem with other software, and your system is using that software, proceed to Step 8.

Step 7 Re-install the patch(es), repeating steps 3 through 6. If your second attempt at downloading and installing the patch(es) succeeds, the procedure is complete. Otherwise, proceed to Step 8.

- Step 8** Contact the Cisco TAC to further analyze the problem and determine a solution. For more information about contacting the Cisco TAC, refer to the “Obtaining Technical Assistance” section on page xviii.

Retrieving Configuration Table Data

You can use the **rtrv-cfg** MML command to retrieve data from the configuration tables. The procedures to retrieve data from the various configuration tables are found in the following sections:

- Retrieving alarm category data, page 3-87
- Retrieving component data, page 3-87
- Retrieving component type data, page 3-88
- Retrieving measurement category data, page 3-88
- Retrieving services data, page 3-88
- Retrieving tables data, page 3-89
- Retrieving default configuration parameters data, page 3-89

Retrieving alarm category data

You can retrieve data from the alarm categories configuration table. To do this, log in to the active Cisco MGC, start an MML session, and enter the following command:

```
rtrv-cfg:alarmcategories
```

The system returns a list of the alarm categories for the Cisco MGC, which begins as follows:

```
MGC-02 - Media Gateway Controller 2001-06-12 15:37:59
M  RTRV
    "Config Fail"
    "XE Rsrc Fail"
    "Gen Fail"
    "SW Fail"
    "SOFTW REQ"
    .
    .
    .
```

For a complete listing of the alarm categories for the Cisco MGC, refer to the *Cisco Media Gateway Controller Software Release 7 Messages Reference Guide*.

Retrieving component data

You can retrieve data from the components configuration table. To do this, log in to the active Cisco MGC, start an MML session, and enter the following command:

```
rtrv-cfg:components
```

The system returns a list of the configured components on the Cisco MGC, which begins as follows:

```
MGC-01 - Media Gateway Controller 2001-06-12 15:00:46
M  RTRV
    "MGC-02: KEY=00010001, PARENT=00000000, DESCR=Media Gateway Controller"
    "CFGG-01: KEY=00020001, PARENT=00010001, DESCR=Config Mgr Subsystem"
    "ALGG-01: KEY=00020002, PARENT=00010001, DESCR=Alarm Mgr Subsystem"
    "MSGG-01: KEY=00020003, PARENT=00010001, DESCR=Measurement Mgr Subsystem"
    "ENGG-01: KEY=00020004, PARENT=00010001, DESCR=Engine Subsystem"
```

```
"IOSG-01: KEY=00020005, PARENT=00010001, DESCR=IO Subsystem"
.
.
.
```

Retrieving component type data

You can retrieve data from the component types configuration table. To do this, log in to the active Cisco MGC, start an MML session, and enter the following command:

```
rtrv-cfg:componenttypes
```

The system returns a list of the component types for the Cisco MGC, which begins as follows:

```
MGC-02 - Media Gateway Controller 2001-06-12 15:24:01
M  RTRV
   "LPC"
   "Proc Group"
   "Proc"
   "Equipment"
   "IO Card"
   .
   .
   .
```

For a complete listing of the component types for the Cisco MGC, refer to the *Cisco Media Gateway Controller Software Release 7 Provisioning Guide*.

Retrieving measurement category data

You can retrieve data from the measurement categories configuration table. To do this, log in to the active Cisco MGC, start an MML session, and enter the following command:

```
rtrv-cfg:meascategories
```

The system returns a list of the measurement categories for the Cisco MGC, which begins as follows:

```
MGC-02 - Media Gateway Controller 2001-06-12 15:26:56
M  RTRV
   "ALL-COUNTERS"
   "LIF-GROUP"
   "LIF: SES"
   "LIF: ES"
   "LIF: CODE VIOLATION"
   .
   .
   .
```

For a complete listing of the measurement categories for the Cisco MGC, refer to the Appendix D, “Cisco Media Gateway Controller Measurements.”

Retrieving services data

You can retrieve data from the services configuration table. To do this, log in to the active Cisco MGC, start an MML session, and enter the following command:

```
rtrv-cfg:services
```

The system returns a list of the services on the Cisco MGC, which begins as follows:

```
MGC-02 - Media Gateway Controller 2001-06-12 15:32:24
```



```

M  RTRV
   "ProcessManagement"
   "ProcessManagement_hi_pri"
   .
   .
   .

```

Retrieving tables data

You can retrieve data from the tables configuration table. To do this, log in to the active Cisco MGC, start an MML session, and enter the following command:

```
rtrv-cfg:tables
```

The system returns a list of the tables for the Cisco MGC, which begins as follows:

```

MGC-02 - Media Gateway Controller 2001-06-12 15:33:47
M  RTRV
   "alarmCategories"
   "componentTypes"
   "components"
   "measCategories"
   "services"
   .
   .
   .

```

Retrieving default configuration parameters data

You can retrieve data from the default configuration parameters table. To do this, log in to the active Cisco MGC, start an MML session, and enter the following command:

```
rtrv-cfg:dfltcfgparms
```

The system returns a list of the default configuration parameters for the Cisco MGC, which begins as follows:

```

MGC-02 - Media Gateway Controller 2001-06-12 15:34:49
M  RTRV
   "*.disableMeas"
   "*.sm_meas_baseaddr"
   "*.platformId"
   .
   .
   .

```

Retrieving the Logging Level of Software Processes

You can use the **rtrv-log** MML command to retrieve the current logging level of a single process or of all of the processes. For more information on processes, refer to “Understanding Processes” section on page 3-4.

To retrieve the current logging level of a single process, log in to the active Cisco MGC, start an MML session, and enter the following command:

```
rtrv-log:process
```

Where *process* is the MML name of the desired process. For a list of valid process names, refer to the “Understanding Processes” section on page 3-4.

For example, to retrieve the current logging level of the call engine process (eng-01), you would enter the following command:

```
rtrv-log:eng-01
```

The system returns a response similar to the following:

```
Media Gateway Controller - MGC-01 2000-01-16 09:38:03
M RTRV
"ENG-01:INFO"
```

To retrieve the current logging level of all of the processes, log in to the active Cisco MGC, start an MML session, and enter the following command:

```
rtrv-log:all
```

The system returns a response similar to the following:

```
Media Gateway Controller - MGC-01 2000-01-16 09:38:03
M RTRV
"ENG-01:INFO"
```



Note

The process manager (PM-01) is not included in the "all" parameter, because this is a special process. To retrieve the logging level of PM-01, it must be used individually, as in the example above.

Managing System Measurements

The operations you can use to manage the Cisco MGC's system measurements are described in the following sections:

- Retrieving Measurements, page 3-90
- Clearing Measurements, page 3-91
- Retrieving Link or Linkset Measurements, page 3-91
- Retrieving SS7 Signaling Point Measurements, page 3-93

Retrieving Measurements

You can view and search the measurements results stored in the measurements log file using the alarm and measurement viewer included in the Cisco MGC viewer toolkit. For more information on viewing and searching measurement files, refer to the “Viewing and Searching System Measurement Files” section on page 3-104.

Each measurement (or counter) is uniquely defined by its measurement category and component identification number. You can retrieve individual measurements using the following MML command from the active Cisco MGC:

```
rtrv-ctr:comp:"meas_cat"
```

Where:

- *comp*—The MML name of the component. A complete list of components can be found in the *Cisco Media Gateway Controller Software Release 7 Provisioning Guide*. You can retrieve a list of system components by entering the **rtrv-cfg:components** MML command.

- *meas_cat*—The desired measurement category. A complete list of measurement categories can be found in Appendix D, “Cisco Media Gateway Controller Measurements”. You can retrieve a list of measurement categories by entering the **rtrv-cfg:meascategories** MML command.

For example, to view the ISUP IAM transmission measurement totals for a component called *dpc1*, enter the following MML command:

```
rtrv-ctr:dpc1:"ISUP: XMIT IAM TOT"
```

The system returns a message similar to the following:

```
MGC-01 - Media Gateway Controller 2000-07-11 10:15:50
M  RTRV
    "dpc1:CAT=\"ISUP: XMIT IAM TOT\",INT=300,VAL=353"
    "dpc1:CAT=\"ISUP: XMIT IAM TOT\",INT=1800,VAL=2501"
```

Clearing Measurements

Each measurement (or counter) is uniquely defined by its measurement category and component identification number. You can retrieve individual measurements using the following MML command from the active Cisco MGC:

```
clr-ctr:comp:"meas_cat"
```

Where:

- *comp*—The MML name of the component. A complete list of components can be found in the *Cisco Media Gateway Controller Software Release 7 Provisioning Guide*. You can retrieve a list of system components by entering the **rtrv-cfg:components** MML command.
- *meas_cat*—The desired measurement category. A complete list of measurement categories can be found in Appendix D, “Cisco Media Gateway Controller Measurements”. You can retrieve a list of measurement categories by entering the **rtrv-cfg:meascategories** MML command.

For example, to clear the ISUP IAM transmission measurement totals for a component called *dpc1*, enter the following MML command:

```
clr-ctr:dpc1:"ISUP: XMIT IAM TOT"
```

Retrieving Link or Linkset Measurements

You can use the **rtrv-lnk-ctr** MML command to retrieve the system measurements for a single link, all the links in a linkset, or all links. For a complete list of system measurements, refer to Appendix D, “Cisco Media Gateway Controller Measurements”.

To retrieve a list of system measurements for a single link, log in to the active Cisco MGC, start an MML session, and enter the following command:

```
rtrv-lnk-ctr:link
```

Where *link* is the MML name of the SS7 link.

For example, to view the measurements for a link called *ls1link1*, you would enter the following command:

```
rtrv-lnk-ctr:ls1link1
```

The system returns a response similar to the following:

```
MGC-03 - Media Gateway Controller 2000-08-22 16:32:23
```

```

M   RTRV
"ls1link1:CAT=\"SC: RCV FRM TOT\",INT=900,VAL=0"
"ls1link1:CAT=\"SC: RCV FRM TOT\",INT=3600,VAL=0"
"ls1link1:CAT=\"SC: RCV FRM TOT\",INT=86400,VAL=0"
"ls1link1:CAT=\"SC: XMIT FRM TOT\",INT=900,VAL=0"
"ls1link1:CAT=\"SC: XMIT FRM TOT\",INT=3600,VAL=0"
"ls1link1:CAT=\"SC: XMIT FRM TOT\",INT=86400,VAL=0"
"ls1link1:CAT=\"SC: RCV BAD TOT\",INT=900,VAL=0"
"ls1link1:CAT=\"SC: RCV BAD TOT\",INT=3600,VAL=0"
"ls1link1:CAT=\"SC: RCV BAD TOT\",INT=86400,VAL=0"
"ls1link1:CAT=\"C7LNK: MSU DROP-CONG\",INT=1800,VAL=0"
"ls1link1:CAT=\"C7LNK: DUR UNAVAIL\",INT=1800,VAL=0"
"ls1link1:CAT=\"SC: RCV BAD CRC\",INT=900,VAL=0"
"ls1link1:CAT=\"SC: RCV BAD CRC\",INT=3600,VAL=0"
"ls1link1:CAT=\"SC: RCV BAD CRC\",INT=86400,VAL=0"
"ls1link1:CAT=\"C7LNK: DUR IS\",INT=1800,VAL=0"
"ls1link1:CAT=\"C7LNK: RCV SIO TOT\",INT=1800,VAL=0"
"ls1link1:CAT=\"C7LNK: XMIT SIO TOT\",INT=1800,VAL=0"
"ls1link1:CAT=\"C7LNK: RCV SU ERR\",INT=1800,VAL=0"

```

To retrieve a list of system measurements for the links that make up a linkset, log in to the active Cisco MGC, start an MML session, and enter the following command:

```
rtrv-lnk-ctr:linkset
```

Where *linkset* is the MML name of the SS7 linkset.

For example, to view the measurements for each link within a linkset called ls1, you would enter the following command:

```
rtrv-lnk-ctr:ls1link1
```

The system returns a response similar to the following:

```

MGC-03 - Media Gateway Controller 2000-08-22 16:32:23
M   RTRV
"ls1link1:CAT=\"SC: RCV FRM TOT\",INT=900,VAL=0"
"ls1link1:CAT=\"SC: RCV FRM TOT\",INT=3600,VAL=0"
"ls1link1:CAT=\"SC: RCV FRM TOT\",INT=86400,VAL=0"
"ls1link1:CAT=\"SC: XMIT FRM TOT\",INT=900,VAL=0"
"ls1link1:CAT=\"SC: XMIT FRM TOT\",INT=3600,VAL=0"
"ls1link1:CAT=\"SC: XMIT FRM TOT\",INT=86400,VAL=0"
"ls1link1:CAT=\"SC: RCV BAD TOT\",INT=900,VAL=0"
"ls1link1:CAT=\"SC: RCV BAD TOT\",INT=3600,VAL=0"
"ls1link1:CAT=\"SC: RCV BAD TOT\",INT=86400,VAL=0"
"ls1link1:CAT=\"C7LNK: MSU DROP-CONG\",INT=1800,VAL=0"
"ls1link1:CAT=\"C7LNK: DUR UNAVAIL\",INT=1800,VAL=0"
"ls1link1:CAT=\"SC: RCV BAD CRC\",INT=900,VAL=0"
"ls1link1:CAT=\"SC: RCV BAD CRC\",INT=3600,VAL=0"
"ls1link1:CAT=\"SC: RCV BAD CRC\",INT=86400,VAL=0"
"ls1link1:CAT=\"C7LNK: DUR IS\",INT=1800,VAL=0"
"ls1link1:CAT=\"C7LNK: RCV SIO TOT\",INT=1800,VAL=0"
"ls1link1:CAT=\"C7LNK: XMIT SIO TOT\",INT=1800,VAL=0"
"ls1link1:CAT=\"C7LNK: RCV SU ERR\",INT=1800,VAL=0"
"ls1link2:CAT=\"SC: RCV FRM TOT\",INT=900,VAL=0"
"ls1link2:CAT=\"SC: RCV FRM TOT\",INT=3600,VAL=0"
"ls1link2:CAT=\"SC: RCV FRM TOT\",INT=86400,VAL=0"
"ls1link2:CAT=\"SC: XMIT FRM TOT\",INT=900,VAL=0"
"ls1link2:CAT=\"SC: XMIT FRM TOT\",INT=3600,VAL=0"
"ls1link2:CAT=\"SC: XMIT FRM TOT\",INT=86400,VAL=0"
"ls1link2:CAT=\"SC: RCV BAD TOT\",INT=900,VAL=0"
"ls1link2:CAT=\"SC: RCV BAD TOT\",INT=3600,VAL=0"
"ls1link2:CAT=\"SC: RCV BAD TOT\",INT=86400,VAL=0"
"ls1link2:CAT=\"C7LNK: MSU DROP-CONG\",INT=1800,VAL=0"

```

```
"ls1link2:CAT=\"C7LNK: DUR UNAVAIL\",INT=1800,VAL=0"
"ls1link2:CAT=\"SC: RCV BAD CRC\",INT=900,VAL=0"
"ls1link2:CAT=\"SC: RCV BAD CRC\",INT=3600,VAL=0"
"ls1link2:CAT=\"SC: RCV BAD CRC\",INT=86400,VAL=0"
"ls1link2:CAT=\"C7LNK: DUR IS\",INT=1800,VAL=0"
"ls1link2:CAT=\"C7LNK: RCV SIO TOT\",INT=1800,VAL=0"
"ls1link2:CAT=\"C7LNK: XMIT SIO TOT\",INT=1800,VAL=0"
"ls1link2:CAT=\"C7LNK: RCV SU ERR\",INT=1800,VAL=0"
```

To retrieve a list of system measurements for all the links on your Cisco MGC, log in to the active Cisco MGC, start an MML session, and enter the following command:

```
rtrv-lnk-ctr:all
```

The system returns a response similar to the following:

```
MGC-03 - Media Gateway Controller 2000-08-22 16:32:23
M RTRV
"ls1link1:CAT=\"SC: RCV FRM TOT\",INT=900,VAL=0"
"ls1link2:CAT=\"SC: RCV FRM TOT\",INT=900,VAL=0"
"ls1link2:CAT=\"SC: RCV FRM TOT\",INT=3600,VAL=0"
"ls1link2:CAT=\"SC: RCV FRM TOT\",INT=86400,VAL=0"
"ls1link2:CAT=\"SC: XMIT FRM TOT\",INT=900,VAL=0"
"ls1link2:CAT=\"SC: XMIT FRM TOT\",INT=3600,VAL=0"
"ls1link2:CAT=\"SC: XMIT FRM TOT\",INT=86400,VAL=0"
"ls1link2:CAT=\"SC: RCV BAD TOT\",INT=900,VAL=0"
"ls1link2:CAT=\"SC: RCV BAD TOT\",INT=3600,VAL=0"
"ls1link2:CAT=\"SC: RCV BAD TOT\",INT=86400,VAL=0"
"ls2link1:CAT=\"SC: RCV FRM TOT\",INT=900,VAL=0"
"ls2link1:CAT=\"SC: RCV FRM TOT\",INT=3600,VAL=0"
"ls2link1:CAT=\"SC: RCV FRM TOT\",INT=86400,VAL=0"
"ls2link1:CAT=\"SC: XMIT FRM TOT\",INT=900,VAL=0"
"ls2link1:CAT=\"SC: XMIT FRM TOT\",INT=3600,VAL=0"
"ls2link1:CAT=\"SC: XMIT FRM TOT\",INT=86400,VAL=0"
"ls2link1:CAT=\"C7LNK: RCV SU ERR\",INT=1800,VAL=0"
"ls2link2:CAT=\"SC: RCV FRM TOT\",INT=900,VAL=0"
"ls2link2:CAT=\"SC: RCV FRM TOT\",INT=3600,VAL=0"
"ls2link2:CAT=\"SC: RCV FRM TOT\",INT=86400,VAL=0"
"ls2link2:CAT=\"SC: XMIT FRM TOT\",INT=900,VAL=0"
"ls2link2:CAT=\"SC: XMIT FRM TOT\",INT=3600,VAL=0"
"ls2link2:CAT=\"SC: XMIT FRM TOT\",INT=86400,VAL=0"
"ls2link2:CAT=\"SC: RCV BAD TOT\",INT=900,VAL=0"
"ls2link2:CAT=\"SC: RCV BAD TOT\",INT=3600,VAL=0"
```

Retrieving SS7 Signaling Point Measurements

You can use the **rtrv-sp-ctr** MML command to retrieve the system measurements for a single SS7 signaling point or for all SS7 signaling points. For a complete list of system measurements, refer to Appendix D, “Cisco Media Gateway Controller Measurements”.

To retrieve a list of system measurements for a single SS7 signaling point, log in to the active Cisco MGC, start an MML session, and enter the following command:

```
rtrv-sp-ctr:point_code
```

Where *point_code* is the MML name of the SS7 signaling point.

For example, to view the measurements for a point code called dpc2, you would enter the following command:

```
rtrv-sp-ctr:dpc2
```

The system returns a response similar to the following:

MGC-02 - Media Gateway Controller 2001-06-13 14:08:39

M RTRV

```
"dpc2:CAT=\"ISUP: XMIT BLA TOT\",INT=300,VAL=0"
"dpc2:CAT=\"ISUP: XMIT BLA TOT\",INT=1800,VAL=0"
"dpc2:CAT=\"ISUP: CHAN MATE UNAVAILABLE\",INT=300,VAL=0"
"dpc2:CAT=\"ISUP: CHAN MATE UNAVAILABLE\",INT=1800,VAL=0"
"dpc2:CAT=\"SP: cInit out\",INT=900,VAL=0"
"dpc2:CAT=\"SP: cInit out\",INT=3600,VAL=0"
"dpc2:CAT=\"SP: cInit out\",INT=86400,VAL=8"
"dpc2:CAT=\"SP: PDU in\",INT=900,VAL=0"
"dpc2:CAT=\"SP: PDU in\",INT=3600,VAL=0"
"dpc2:CAT=\"SP: PDU in\",INT=86400,VAL=50"
"dpc2:CAT=\"ISUP: XMIT CGB TOT\",INT=300,VAL=0"
"dpc2:CAT=\"ISUP: XMIT CGB TOT\",INT=1800,VAL=0"
"dpc2:CAT=\"ISUP: RCV BLA TOT\",INT=300,VAL=0"
"dpc2:CAT=\"ISUP: RCV BLA TOT\",INT=1800,VAL=0"
"dpc2:CAT=\"ISUP: XMIT CQR TOT\",INT=300,VAL=0"
"dpc2:CAT=\"ISUP: XMIT CQR TOT\",INT=1800,VAL=0"
"dpc2:CAT=\"ISUP: RCV CQM TOT\",INT=300,VAL=0"
"dpc2:CAT=\"ISUP: RCV CQM TOT\",INT=1800,VAL=0"
"dpc2:CAT=\"ISUP: XMIT CVR TOT\",INT=300,VAL=0"
"dpc2:CAT=\"ISUP: XMIT CVR TOT\",INT=1800,VAL=0"
"dpc2:CAT=\"ISUP: RCV LPA TOT\",INT=300,VAL=0"
"dpc2:CAT=\"ISUP: RCV LPA TOT\",INT=1800,VAL=0"
"dpc2:CAT=\"ISUP: XMIT RSC TOT\",INT=300,VAL=0"
"dpc2:CAT=\"ISUP: XMIT RSC TOT\",INT=1800,VAL=0"
"dpc2:CAT=\"ISUP: XMIT ACM TOT\",INT=300,VAL=0"
"dpc2:CAT=\"ISUP: XMIT ACM TOT\",INT=1800,VAL=0"
"dpc2:CAT=\"ISUP: XMIT UBA TOT\",INT=300,VAL=0"
"dpc2:CAT=\"ISUP: XMIT UBA TOT\",INT=1800,VAL=0"
"dpc2:CAT=\"ISUP: XMIT MSG TOT\",INT=300,VAL=0"
"dpc2:CAT=\"ISUP: XMIT MSG TOT\",INT=1800,VAL=0"
"dpc2:CAT=\"ISUP: XMIT CCR TOT\",INT=300,VAL=0"
"dpc2:CAT=\"ISUP: XMIT CCR TOT\",INT=1800,VAL=0"
"dpc2:CAT=\"ISUP: RCV UBA TOT\",INT=300,VAL=0"
"dpc2:CAT=\"ISUP: RCV UBA TOT\",INT=1800,VAL=0"
"dpc2:CAT=\"ISUP: RCV MSG TOT\",INT=300,VAL=0"
"dpc2:CAT=\"ISUP: RCV MSG TOT\",INT=1800,VAL=0"
"dpc2:CAT=\"ISUP: UNEX MSG TOT\",INT=300,VAL=0"
"dpc2:CAT=\"ISUP: UNEX MSG TOT\",INT=1800,VAL=0"
"dpc2:CAT=\"ISUP: XMIT IAM TOT\",INT=300,VAL=0"
"dpc2:CAT=\"ISUP: XMIT IAM TOT\",INT=1800,VAL=0"
"dpc2:CAT=\"ISUP: RCV IAM TOT\",INT=300,VAL=0"
"dpc2:CAT=\"ISUP: RCV IAM TOT\",INT=1800,VAL=0"
"dpc2:CAT=\"ISUP: UNREC MSG TOT\",INT=300,VAL=0"
"dpc2:CAT=\"ISUP: UNREC MSG TOT\",INT=1800,VAL=0"
"dpc2:CAT=\"ISUP: RCV CFN TOT\",INT=300,VAL=0"
"dpc2:CAT=\"ISUP: RCV CFN TOT\",INT=1800,VAL=0"
"dpc2:CAT=\"ISUP: RCV CCR TOT\",INT=300,VAL=0"
"dpc2:CAT=\"ISUP: RCV CCR TOT\",INT=1800,VAL=0"
"dpc2:CAT=\"ISUP: XMIT ANM TOT\",INT=300,VAL=0"
"dpc2:CAT=\"ISUP: XMIT ANM TOT\",INT=1800,VAL=0"
"dpc2:CAT=\"ISUP: XMIT COT TOT\",INT=300,VAL=0"
"dpc2:CAT=\"ISUP: XMIT COT TOT\",INT=1800,VAL=0"
"dpc2:CAT=\"ISUP: RCV ANM TOT\",INT=300,VAL=0"
"dpc2:CAT=\"ISUP: RCV ANM TOT\",INT=1800,VAL=0"
"dpc2:CAT=\"ISUP: RCV INR TOT\",INT=300,VAL=0"
"dpc2:CAT=\"ISUP: RCV INR TOT\",INT=1800,VAL=0"
"dpc2:CAT=\"ISUP: RCV COT TOT\",INT=300,VAL=0"
"dpc2:CAT=\"ISUP: RCV COT TOT\",INT=1800,VAL=0"
"dpc2:CAT=\"ISUP: XMIT BLO TOT\",INT=300,VAL=0"
"dpc2:CAT=\"ISUP: XMIT BLO TOT\",INT=1800,VAL=0"
```

```

"dpc2:CAT=\"ISUP: ABN REL TOT\",INT=300,VAL=0"
"dpc2:CAT=\"ISUP: ABN REL TOT\",INT=1800,VAL=0"
"dpc2:CAT=\"ISUP: XMIT REL TOT\",INT=300,VAL=0"
"dpc2:CAT=\"ISUP: XMIT REL TOT\",INT=1800,VAL=0"
"dpc2:CAT=\"ISUP: RCV CVR TOT\",INT=300,VAL=0"
"dpc2:CAT=\"ISUP: RCV CVR TOT\",INT=1800,VAL=0"
"dpc2:CAT=\"ISUP: RCV CGU TOT\",INT=300,VAL=0"
"dpc2:CAT=\"ISUP: RCV CGU TOT\",INT=1800,VAL=0"
"dpc2:CAT=\"ISUP: XMIT SUS TOT\",INT=300,VAL=0"
"dpc2:CAT=\"ISUP: XMIT SUS TOT\",INT=1800,VAL=0"
"dpc2:CAT=\"ISUP: XMIT CVT TOT\",INT=300,VAL=0"
"dpc2:CAT=\"ISUP: XMIT CVT TOT\",INT=1800,VAL=0"
"dpc2:CAT=\"ISUP: XMIT GRA TOT\",INT=300,VAL=0"
"dpc2:CAT=\"ISUP: XMIT GRA TOT\",INT=1800,VAL=0"
"dpc2:CAT=\"ISUP: RCV SUS TOT\",INT=300,VAL=0"
"dpc2:CAT=\"ISUP: RCV SUS TOT\",INT=1800,VAL=0"
"dpc2:CAT=\"ISUP: RCV FOT TOT\",INT=300,VAL=0"
"dpc2:CAT=\"ISUP: RCV FOT TOT\",INT=1800,VAL=0"
"dpc2:CAT=\"ISUP: RCV GRS TOT\",INT=300,VAL=0"
"dpc2:CAT=\"ISUP: RCV GRS TOT\",INT=1800,VAL=0"
"dpc2:CAT=\"ISUP: XMIT CFN TOT\",INT=300,VAL=0"
"dpc2:CAT=\"ISUP: XMIT CFN TOT\",INT=1800,VAL=0"
"dpc2:CAT=\"ISUP: XMIT UBL TOT\",INT=300,VAL=0"
"dpc2:CAT=\"ISUP: XMIT UBL TOT\",INT=1800,VAL=0"
"dpc2:CAT=\"ISUP: RCV CVT TOT\",INT=300,VAL=0"
"dpc2:CAT=\"ISUP: RCV CVT TOT\",INT=1800,VAL=0"
"dpc2:CAT=\"ISUP: XMIT LPA TOT\",INT=300,VAL=0"
"dpc2:CAT=\"ISUP: XMIT LPA TOT\",INT=1800,VAL=0"
"dpc2:CAT=\"ISUP: XMIT FAC TOT\",INT=300,VAL=0"
"dpc2:CAT=\"ISUP: XMIT FAC TOT\",INT=1800,VAL=0"
"dpc2:CAT=\"ISUP: RCV FAC TOT\",INT=300,VAL=0"
"dpc2:CAT=\"ISUP: RCV FAC TOT\",INT=1800,VAL=0"
"dpc2:CAT=\"ISUP: RCV CGUA TOT\",INT=300,VAL=0"
"dpc2:CAT=\"ISUP: RCV CGUA TOT\",INT=1800,VAL=0"
"dpc2:CAT=\"ISUP: RCV UBL TOT\",INT=300,VAL=0"
"dpc2:CAT=\"ISUP: RCV UBL TOT\",INT=1800,VAL=0"
"dpc2:CAT=\"ISUP: XMIT USR TOT\",INT=300,VAL=0"
"dpc2:CAT=\"ISUP: XMIT USR TOT\",INT=1800,VAL=0"
"dpc2:CAT=\"ISUP: XMIT CGUA TOT\",INT=300,VAL=0"
"dpc2:CAT=\"ISUP: XMIT CGUA TOT\",INT=1800,VAL=0"
"dpc2:CAT=\"ISUP: RCV USR TOT\",INT=300,VAL=0"
"dpc2:CAT=\"ISUP: RCV USR TOT\",INT=1800,VAL=0"
"dpc2:CAT=\"ISUP: RCV ACM TOT\",INT=300,VAL=0"
"dpc2:CAT=\"ISUP: RCV ACM TOT\",INT=1800,VAL=0"
"dpc2:CAT=\"ISUP: XMIT FOT TOT\",INT=300,VAL=0"
"dpc2:CAT=\"ISUP: XMIT FOT TOT\",INT=1800,VAL=0"
"dpc2:CAT=\"ISUP: XMIT PAM TOT\",INT=300,VAL=0"
"dpc2:CAT=\"ISUP: XMIT PAM TOT\",INT=1800,VAL=0"
"dpc2:CAT=\"ISUP: RCV CGB TOT\",INT=300,VAL=0"
"dpc2:CAT=\"ISUP: RCV CGB TOT\",INT=1800,VAL=0"
"dpc2:CAT=\"ISUP: RCV RLC TOT\",INT=300,VAL=0"
"dpc2:CAT=\"ISUP: RCV RLC TOT\",INT=1800,VAL=0"
"dpc2:CAT=\"ISUP: RCV REL TOT\",INT=300,VAL=0"
"dpc2:CAT=\"ISUP: RCV REL TOT\",INT=1800,VAL=0"
"dpc2:CAT=\"ISUP: RCV CRM TOT\",INT=300,VAL=0"
"dpc2:CAT=\"ISUP: RCV CRM TOT\",INT=1800,VAL=0"
"dpc2:CAT=\"ISUP: XMIT CGBA TOT\",INT=300,VAL=0"
"dpc2:CAT=\"ISUP: XMIT CGBA TOT\",INT=1800,VAL=0"
"dpc2:CAT=\"ISUP: XMIT RLC TOT\",INT=300,VAL=0"
"dpc2:CAT=\"ISUP: XMIT RLC TOT\",INT=1800,VAL=0"
"dpc2:CAT=\"C7SP: SP DUR UNAVAIL\",INT=300,VAL=0"
"dpc2:CAT=\"C7SP: SP DUR UNAVAIL\",INT=1800,VAL=0"
"dpc2:CAT=\"ISUP: XMIT CRM TOT\",INT=300,VAL=0"
"dpc2:CAT=\"ISUP: XMIT CRM TOT\",INT=1800,VAL=0"

```

```

"dpc2:CAT=\"ISUP: RCV UCIC TOT\",INT=300,VAL=0"
"dpc2:CAT=\"ISUP: RCV UCIC TOT\",INT=1800,VAL=0"
"dpc2:CAT=\"ISUP: RCV CGBA TOT\",INT=300,VAL=0"
"dpc2:CAT=\"ISUP: RCV CGBA TOT\",INT=1800,VAL=0"
"dpc2:CAT=\"C7SP: XMIT MSU DROP/RTE\",INT=1800,VAL=0"
"dpc2:CAT=\"ISUP: XMIT GRS TOT\",INT=300,VAL=0"
"dpc2:CAT=\"ISUP: XMIT GRS TOT\",INT=1800,VAL=0"
"dpc2:CAT=\"ISUP: RCV RSC TOT\",INT=300,VAL=0"
"dpc2:CAT=\"ISUP: RCV RSC TOT\",INT=1800,VAL=0"
"dpc2:CAT=\"ISUP: XMIT RES TOT\",INT=300,VAL=0"
"dpc2:CAT=\"ISUP: XMIT RES TOT\",INT=1800,VAL=0"
"dpc2:CAT=\"ISUP: XMIT UCIC TOT\",INT=300,VAL=0"
"dpc2:CAT=\"ISUP: XMIT UCIC TOT\",INT=1800,VAL=0"
"dpc2:CAT=\"ISUP: RCV RES TOT\",INT=300,VAL=0"
"dpc2:CAT=\"ISUP: RCV RES TOT\",INT=1800,VAL=0"
"dpc2:CAT=\"ISUP: RCV PAM TOT\",INT=300,VAL=0"
"dpc2:CAT=\"ISUP: RCV PAM TOT\",INT=1800,VAL=0"
"dpc2:CAT=\"ISUP: RCV GRA TOT\",INT=300,VAL=0"
"dpc2:CAT=\"ISUP: RCV GRA TOT\",INT=1800,VAL=0"
"dpc2:CAT=\"ISUP: XMIT EXM TOT\",INT=300,VAL=0"
"dpc2:CAT=\"ISUP: XMIT EXM TOT\",INT=1800,VAL=0"
"dpc2:CAT=\"ISUP: XMIT CGU TOT\",INT=300,VAL=0"
"dpc2:CAT=\"ISUP: XMIT CGU TOT\",INT=1800,VAL=0"
"dpc2:CAT=\"ISUP: RCV EXM TOT\",INT=300,VAL=0"
"dpc2:CAT=\"ISUP: RCV EXM TOT\",INT=1800,VAL=0"
"dpc2:CAT=\"ISUP: XMIT INF TOT\",INT=300,VAL=0"
"dpc2:CAT=\"ISUP: XMIT INF TOT\",INT=1800,VAL=0"
"dpc2:CAT=\"ISUP: XMIT CQM TOT\",INT=300,VAL=0"
"dpc2:CAT=\"ISUP: XMIT CQM TOT\",INT=1800,VAL=0"
"dpc2:CAT=\"ISUP: RCV INF TOT\",INT=300,VAL=0"
"dpc2:CAT=\"ISUP: RCV INF TOT\",INT=1800,VAL=0"
"dpc2:CAT=\"ISUP: RCV BLO TOT\",INT=300,VAL=0"
"dpc2:CAT=\"ISUP: RCV BLO TOT\",INT=1800,VAL=0"
"dpc2:CAT=\"SP: cInit in\",INT=900,VAL=0"
"dpc2:CAT=\"SP: cInit in\",INT=3600,VAL=0"
"dpc2:CAT=\"SP: cInit in\",INT=86400,VAL=17"
"dpc2:CAT=\"ISUP: XMIT CPG TOT\",INT=300,VAL=0"
"dpc2:CAT=\"ISUP: XMIT CPG TOT\",INT=1800,VAL=0"
"dpc2:CAT=\"SP: PDU out\",INT=900,VAL=0"
"dpc2:CAT=\"SP: PDU out\",INT=3600,VAL=0"
"dpc2:CAT=\"SP: PDU out\",INT=86400,VAL=99"
"dpc2:CAT=\"ISUP: RCV CQR TOT\",INT=300,VAL=0"
"dpc2:CAT=\"ISUP: RCV CQR TOT\",INT=1800,VAL=0"
"dpc2:CAT=\"ISUP: XMIT CRA TOT\",INT=300,VAL=0"
"dpc2:CAT=\"ISUP: XMIT CRA TOT\",INT=1800,VAL=0"
"dpc2:CAT=\"ISUP: RCV CPG TOT\",INT=300,VAL=0"
"dpc2:CAT=\"ISUP: RCV CPG TOT\",INT=1800,VAL=0"
"dpc2:CAT=\"ISUP: XMIT INR TOT\",INT=300,VAL=0"
"dpc2:CAT=\"ISUP: XMIT INR TOT\",INT=1800,VAL=0"
"dpc2:CAT=\"ISUP: RCV CRA TOT\",INT=300,VAL=0"
"dpc2:CAT=\"ISUP: RCV CRA TOT\",INT=1800,VAL=0"

```

To retrieve a list of system measurements for all the SS7 signaling points on your Cisco MGC, log in to the active Cisco MGC, start an MML session, and enter the following command:

```
rtrv-sp-ctr:all
```

The system returns a response similar to the following:

```

MGC-02 - Media Gateway Controller 2001-06-13 14:08:39
M RTRV
"opc2"
/* No active counters found for this component/category */
"dpc2:CAT=\"ISUP: XMIT BLA TOT\",INT=300,VAL=0"

```



```

"dpc2:CAT=\"ISUP: XMIT BLA TOT\",INT=1800,VAL=0"
"dpc2:CAT=\"ISUP: CHAN MATE UNAVAILABLE\",INT=300,VAL=0"
"dpc2:CAT=\"ISUP: CHAN MATE UNAVAILABLE\",INT=1800,VAL=0"
"dpc2:CAT=\"SP: cInit out\",INT=900,VAL=0"
"dpc2:CAT=\"SP: cInit out\",INT=3600,VAL=0"
"dpc2:CAT=\"SP: cInit out\",INT=86400,VAL=8"
"dpc2:CAT=\"SP: PDU in\",INT=900,VAL=0"
"dpc2:CAT=\"SP: PDU in\",INT=3600,VAL=0"
"dpc2:CAT=\"SP: PDU in\",INT=86400,VAL=50"
"dpc2:CAT=\"ISUP: XMIT CGB TOT\",INT=300,VAL=0"
"dpc2:CAT=\"ISUP: XMIT CGB TOT\",INT=1800,VAL=0"
"dpc2:CAT=\"ISUP: RCV BLA TOT\",INT=300,VAL=0"
"dpc2:CAT=\"ISUP: RCV BLA TOT\",INT=1800,VAL=0"
"dpc2:CAT=\"ISUP: XMIT CQR TOT\",INT=300,VAL=0"
"dpc2:CAT=\"ISUP: XMIT CQR TOT\",INT=1800,VAL=0"
"dpc2:CAT=\"ISUP: RCV CQM TOT\",INT=300,VAL=0"
"dpc2:CAT=\"ISUP: RCV CQM TOT\",INT=1800,VAL=0"
"dpc2:CAT=\"ISUP: XMIT CVR TOT\",INT=300,VAL=0"
"dpc2:CAT=\"ISUP: XMIT CVR TOT\",INT=1800,VAL=0"
"dpc2:CAT=\"ISUP: RCV LPA TOT\",INT=300,VAL=0"
"dpc2:CAT=\"ISUP: RCV LPA TOT\",INT=1800,VAL=0"
"dpc2:CAT=\"ISUP: XMIT RSC TOT\",INT=300,VAL=0"
"dpc2:CAT=\"ISUP: XMIT RSC TOT\",INT=1800,VAL=0"
"dpc2:CAT=\"ISUP: XMIT ACM TOT\",INT=300,VAL=0"
"dpc2:CAT=\"ISUP: XMIT ACM TOT\",INT=1800,VAL=0"
"dpc2:CAT=\"ISUP: XMIT UBA TOT\",INT=300,VAL=0"
"dpc2:CAT=\"ISUP: XMIT UBA TOT\",INT=1800,VAL=0"
"dpc2:CAT=\"ISUP: XMIT MSG TOT\",INT=300,VAL=0"
"dpc2:CAT=\"ISUP: XMIT MSG TOT\",INT=1800,VAL=0"
"dpc2:CAT=\"ISUP: XMIT CCR TOT\",INT=300,VAL=0"
"dpc2:CAT=\"ISUP: XMIT CCR TOT\",INT=1800,VAL=0"
"dpc2:CAT=\"ISUP: RCV UBA TOT\",INT=300,VAL=0"
"dpc2:CAT=\"ISUP: RCV UBA TOT\",INT=1800,VAL=0"
"dpc2:CAT=\"ISUP: RCV MSG TOT\",INT=300,VAL=0"
"dpc2:CAT=\"ISUP: RCV MSG TOT\",INT=1800,VAL=0"
"dpc2:CAT=\"ISUP: UNEX MSG TOT\",INT=300,VAL=0"
"dpc2:CAT=\"ISUP: UNEX MSG TOT\",INT=1800,VAL=0"
"dpc2:CAT=\"ISUP: XMIT IAM TOT\",INT=300,VAL=0"
"dpc2:CAT=\"ISUP: XMIT IAM TOT\",INT=1800,VAL=0"
"dpc2:CAT=\"ISUP: RCV IAM TOT\",INT=300,VAL=0"
"dpc2:CAT=\"ISUP: RCV IAM TOT\",INT=1800,VAL=0"
"dpc2:CAT=\"ISUP: UNREC MSG TOT\",INT=300,VAL=0"
"dpc2:CAT=\"ISUP: UNREC MSG TOT\",INT=1800,VAL=0"
"dpc2:CAT=\"ISUP: RCV CFN TOT\",INT=300,VAL=0"
"dpc2:CAT=\"ISUP: RCV CFN TOT\",INT=1800,VAL=0"
"dpc2:CAT=\"ISUP: RCV CCR TOT\",INT=300,VAL=0"
"dpc2:CAT=\"ISUP: RCV CCR TOT\",INT=1800,VAL=0"
"dpc2:CAT=\"ISUP: XMIT ANM TOT\",INT=300,VAL=0"
"dpc2:CAT=\"ISUP: XMIT ANM TOT\",INT=1800,VAL=0"
"dpc2:CAT=\"ISUP: XMIT COT TOT\",INT=300,VAL=0"
"dpc2:CAT=\"ISUP: XMIT COT TOT\",INT=1800,VAL=0"
"dpc2:CAT=\"ISUP: RCV ANM TOT\",INT=300,VAL=0"
"dpc2:CAT=\"ISUP: RCV ANM TOT\",INT=1800,VAL=0"
"dpc2:CAT=\"ISUP: RCV INR TOT\",INT=300,VAL=0"
"dpc2:CAT=\"ISUP: RCV INR TOT\",INT=1800,VAL=0"
"dpc2:CAT=\"ISUP: RCV COT TOT\",INT=300,VAL=0"
"dpc2:CAT=\"ISUP: RCV COT TOT\",INT=1800,VAL=0"
"dpc2:CAT=\"ISUP: XMIT BLO TOT\",INT=300,VAL=0"
"dpc2:CAT=\"ISUP: XMIT BLO TOT\",INT=1800,VAL=0"
"dpc2:CAT=\"ISUP: ABN REL TOT\",INT=300,VAL=0"
"dpc2:CAT=\"ISUP: ABN REL TOT\",INT=1800,VAL=0"
"dpc2:CAT=\"ISUP: XMIT REL TOT\",INT=300,VAL=0"
"dpc2:CAT=\"ISUP: XMIT REL TOT\",INT=1800,VAL=0"
"dpc2:CAT=\"ISUP: RCV CVR TOT\",INT=300,VAL=0"

```

```

"dpc2:CAT=\"ISUP: RCV CVR TOT\",INT=1800,VAL=0"
"dpc2:CAT=\"ISUP: RCV CGU TOT\",INT=300,VAL=0"
"dpc2:CAT=\"ISUP: RCV CGU TOT\",INT=1800,VAL=0"
"dpc2:CAT=\"ISUP: XMIT SUS TOT\",INT=300,VAL=0"
"dpc2:CAT=\"ISUP: XMIT SUS TOT\",INT=1800,VAL=0"
"dpc2:CAT=\"ISUP: XMIT CVT TOT\",INT=300,VAL=0"
"dpc2:CAT=\"ISUP: XMIT CVT TOT\",INT=1800,VAL=0"
"dpc2:CAT=\"ISUP: XMIT GRA TOT\",INT=300,VAL=0"
"dpc2:CAT=\"ISUP: XMIT GRA TOT\",INT=1800,VAL=0"
"dpc2:CAT=\"ISUP: RCV SUS TOT\",INT=300,VAL=0"
"dpc2:CAT=\"ISUP: RCV SUS TOT\",INT=1800,VAL=0"
"dpc2:CAT=\"ISUP: RCV FOT TOT\",INT=300,VAL=0"
"dpc2:CAT=\"ISUP: RCV FOT TOT\",INT=1800,VAL=0"
"dpc2:CAT=\"ISUP: RCV GRS TOT\",INT=300,VAL=0"
"dpc2:CAT=\"ISUP: RCV GRS TOT\",INT=1800,VAL=0"
"dpc2:CAT=\"ISUP: XMIT CFN TOT\",INT=300,VAL=0"
"dpc2:CAT=\"ISUP: XMIT CFN TOT\",INT=1800,VAL=0"
"dpc2:CAT=\"ISUP: XMIT UBL TOT\",INT=300,VAL=0"
"dpc2:CAT=\"ISUP: XMIT UBL TOT\",INT=1800,VAL=0"
"dpc2:CAT=\"ISUP: RCV CVT TOT\",INT=300,VAL=0"
"dpc2:CAT=\"ISUP: RCV CVT TOT\",INT=1800,VAL=0"
"dpc2:CAT=\"ISUP: XMIT LPA TOT\",INT=300,VAL=0"
"dpc2:CAT=\"ISUP: XMIT LPA TOT\",INT=1800,VAL=0"
"dpc2:CAT=\"ISUP: XMIT FAC TOT\",INT=300,VAL=0"
"dpc2:CAT=\"ISUP: XMIT FAC TOT\",INT=1800,VAL=0"
"dpc2:CAT=\"ISUP: RCV FAC TOT\",INT=300,VAL=0"
"dpc2:CAT=\"ISUP: RCV FAC TOT\",INT=1800,VAL=0"
"dpc2:CAT=\"ISUP: RCV CGUA TOT\",INT=300,VAL=0"
"dpc2:CAT=\"ISUP: RCV CGUA TOT\",INT=1800,VAL=0"
"dpc2:CAT=\"ISUP: RCV UBL TOT\",INT=300,VAL=0"
"dpc2:CAT=\"ISUP: RCV UBL TOT\",INT=1800,VAL=0"
"dpc2:CAT=\"ISUP: XMIT USR TOT\",INT=300,VAL=0"
"dpc2:CAT=\"ISUP: XMIT USR TOT\",INT=1800,VAL=0"
"dpc2:CAT=\"ISUP: XMIT CGUA TOT\",INT=300,VAL=0"
"dpc2:CAT=\"ISUP: XMIT CGUA TOT\",INT=1800,VAL=0"
"dpc2:CAT=\"ISUP: RCV USR TOT\",INT=300,VAL=0"
"dpc2:CAT=\"ISUP: RCV USR TOT\",INT=1800,VAL=0"
"dpc2:CAT=\"ISUP: RCV ACM TOT\",INT=300,VAL=0"
"dpc2:CAT=\"ISUP: RCV ACM TOT\",INT=1800,VAL=0"
"dpc2:CAT=\"ISUP: XMIT FOT TOT\",INT=300,VAL=0"
"dpc2:CAT=\"ISUP: XMIT FOT TOT\",INT=1800,VAL=0"
"dpc2:CAT=\"ISUP: XMIT PAM TOT\",INT=300,VAL=0"
"dpc2:CAT=\"ISUP: XMIT PAM TOT\",INT=1800,VAL=0"
"dpc2:CAT=\"ISUP: RCV CGB TOT\",INT=300,VAL=0"
"dpc2:CAT=\"ISUP: RCV CGB TOT\",INT=1800,VAL=0"
"dpc2:CAT=\"ISUP: RCV RLC TOT\",INT=300,VAL=0"
"dpc2:CAT=\"ISUP: RCV RLC TOT\",INT=1800,VAL=0"
"dpc2:CAT=\"ISUP: RCV REL TOT\",INT=300,VAL=0"
"dpc2:CAT=\"ISUP: RCV REL TOT\",INT=1800,VAL=0"
"dpc2:CAT=\"ISUP: RCV CRM TOT\",INT=300,VAL=0"
"dpc2:CAT=\"ISUP: RCV CRM TOT\",INT=1800,VAL=0"
"dpc2:CAT=\"ISUP: XMIT CGBA TOT\",INT=300,VAL=0"
"dpc2:CAT=\"ISUP: XMIT CGBA TOT\",INT=1800,VAL=0"
"dpc2:CAT=\"ISUP: XMIT RLC TOT\",INT=300,VAL=0"
"dpc2:CAT=\"ISUP: XMIT RLC TOT\",INT=1800,VAL=0"
"dpc2:CAT=\"C7SP: SP DUR UNAVAIL\",INT=300,VAL=0"
"dpc2:CAT=\"C7SP: SP DUR UNAVAIL\",INT=1800,VAL=0"
"dpc2:CAT=\"ISUP: XMIT CRM TOT\",INT=300,VAL=0"
"dpc2:CAT=\"ISUP: XMIT CRM TOT\",INT=1800,VAL=0"
"dpc2:CAT=\"ISUP: RCV UCIC TOT\",INT=300,VAL=0"
"dpc2:CAT=\"ISUP: RCV UCIC TOT\",INT=1800,VAL=0"
"dpc2:CAT=\"ISUP: RCV CGBA TOT\",INT=300,VAL=0"
"dpc2:CAT=\"ISUP: RCV CGBA TOT\",INT=1800,VAL=0"
"dpc2:CAT=\"C7SP: XMIT MSU DROP/RTE\",INT=1800,VAL=0"

```

```

"dpc2:CAT=\"ISUP: XMIT GRS TOT\",INT=300,VAL=0"
"dpc2:CAT=\"ISUP: XMIT GRS TOT\",INT=1800,VAL=0"
"dpc2:CAT=\"ISUP: RCV RSC TOT\",INT=300,VAL=0"
"dpc2:CAT=\"ISUP: RCV RSC TOT\",INT=1800,VAL=0"
"dpc2:CAT=\"ISUP: XMIT RES TOT\",INT=300,VAL=0"
"dpc2:CAT=\"ISUP: XMIT RES TOT\",INT=1800,VAL=0"
"dpc2:CAT=\"ISUP: XMIT UCIC TOT\",INT=300,VAL=0"
"dpc2:CAT=\"ISUP: XMIT UCIC TOT\",INT=1800,VAL=0"
"dpc2:CAT=\"ISUP: RCV RES TOT\",INT=300,VAL=0"
"dpc2:CAT=\"ISUP: RCV RES TOT\",INT=1800,VAL=0"
"dpc2:CAT=\"ISUP: RCV PAM TOT\",INT=300,VAL=0"
"dpc2:CAT=\"ISUP: RCV PAM TOT\",INT=1800,VAL=0"
"dpc2:CAT=\"ISUP: RCV GRA TOT\",INT=300,VAL=0"
"dpc2:CAT=\"ISUP: RCV GRA TOT\",INT=1800,VAL=0"
"dpc2:CAT=\"ISUP: XMIT EXM TOT\",INT=300,VAL=0"
"dpc2:CAT=\"ISUP: XMIT EXM TOT\",INT=1800,VAL=0"
"dpc2:CAT=\"ISUP: XMIT CGU TOT\",INT=300,VAL=0"
"dpc2:CAT=\"ISUP: XMIT CGU TOT\",INT=1800,VAL=0"
"dpc2:CAT=\"ISUP: RCV EXM TOT\",INT=300,VAL=0"
"dpc2:CAT=\"ISUP: RCV EXM TOT\",INT=1800,VAL=0"
"dpc2:CAT=\"ISUP: XMIT INF TOT\",INT=300,VAL=0"
"dpc2:CAT=\"ISUP: XMIT INF TOT\",INT=1800,VAL=0"
"dpc2:CAT=\"ISUP: XMIT CQM TOT\",INT=300,VAL=0"
"dpc2:CAT=\"ISUP: XMIT CQM TOT\",INT=1800,VAL=0"
"dpc2:CAT=\"ISUP: RCV INF TOT\",INT=300,VAL=0"
"dpc2:CAT=\"ISUP: RCV INF TOT\",INT=1800,VAL=0"
"dpc2:CAT=\"ISUP: RCV BLO TOT\",INT=300,VAL=0"
"dpc2:CAT=\"ISUP: RCV BLO TOT\",INT=1800,VAL=0"
"dpc2:CAT=\"SP: cInit in\",INT=900,VAL=0"
"dpc2:CAT=\"SP: cInit in\",INT=3600,VAL=0"
"dpc2:CAT=\"SP: cInit in\",INT=86400,VAL=17"
"dpc2:CAT=\"ISUP: XMIT CPG TOT\",INT=300,VAL=0"
"dpc2:CAT=\"ISUP: XMIT CPG TOT\",INT=1800,VAL=0"
"dpc2:CAT=\"SP: PDU out\",INT=900,VAL=0"
"dpc2:CAT=\"SP: PDU out\",INT=3600,VAL=0"
"dpc2:CAT=\"SP: PDU out\",INT=86400,VAL=99"
"dpc2:CAT=\"ISUP: RCV CQR TOT\",INT=300,VAL=0"
"dpc2:CAT=\"ISUP: RCV CQR TOT\",INT=1800,VAL=0"
"dpc2:CAT=\"ISUP: XMIT CRA TOT\",INT=300,VAL=0"
"dpc2:CAT=\"ISUP: XMIT CRA TOT\",INT=1800,VAL=0"
"dpc2:CAT=\"ISUP: RCV CPG TOT\",INT=300,VAL=0"
"dpc2:CAT=\"ISUP: RCV CPG TOT\",INT=1800,VAL=0"
"dpc2:CAT=\"ISUP: XMIT INR TOT\",INT=300,VAL=0"
"dpc2:CAT=\"ISUP: XMIT INR TOT\",INT=1800,VAL=0"
"dpc2:CAT=\"ISUP: RCV CRA TOT\",INT=300,VAL=0"
"dpc2:CAT=\"ISUP: RCV CRA TOT\",INT=1800,VAL=0"
"opc1"
/* No active counters found for this component/category */
"dpc1:CAT=\"ISUP: XMIT BLA TOT\",INT=300,VAL=0"
"dpc1:CAT=\"ISUP: XMIT BLA TOT\",INT=1800,VAL=0"
"dpc1:CAT=\"ISUP: CHAN MATE UNAVAILABLE\",INT=300,VAL=0"
"dpc1:CAT=\"ISUP: CHAN MATE UNAVAILABLE\",INT=1800,VAL=0"
"dpc1:CAT=\"SP: cInit out\",INT=900,VAL=0"
"dpc1:CAT=\"SP: cInit out\",INT=3600,VAL=0"
"dpc1:CAT=\"SP: cInit out\",INT=86400,VAL=1"
"dpc1:CAT=\"SP: PDU in\",INT=900,VAL=0"
"dpc1:CAT=\"SP: PDU in\",INT=3600,VAL=0"
"dpc1:CAT=\"SP: PDU in\",INT=86400,VAL=13"
"dpc1:CAT=\"ISUP: XMIT CGB TOT\",INT=300,VAL=0"
"dpc1:CAT=\"ISUP: XMIT CGB TOT\",INT=1800,VAL=0"
"dpc1:CAT=\"ISUP: RCV BLA TOT\",INT=300,VAL=0"
"dpc1:CAT=\"ISUP: RCV BLA TOT\",INT=1800,VAL=0"
"dpc1:CAT=\"ISUP: XMIT CQR TOT\",INT=300,VAL=0"
"dpc1:CAT=\"ISUP: XMIT CQR TOT\",INT=1800,VAL=0"

```

```

"dpc1:CAT=\"ISUP: RCV CQM TOT\",INT=300,VAL=0"
"dpc1:CAT=\"ISUP: RCV CQM TOT\",INT=1800,VAL=0"
"dpc1:CAT=\"ISUP: XMIT CVR TOT\",INT=300,VAL=0"
"dpc1:CAT=\"ISUP: XMIT CVR TOT\",INT=1800,VAL=0"
"dpc1:CAT=\"ISUP: RCV LPA TOT\",INT=300,VAL=0"
"dpc1:CAT=\"ISUP: RCV LPA TOT\",INT=1800,VAL=0"
"dpc1:CAT=\"ISUP: XMIT RSC TOT\",INT=300,VAL=0"
"dpc1:CAT=\"ISUP: XMIT RSC TOT\",INT=1800,VAL=0"
"dpc1:CAT=\"ISUP: XMIT ACM TOT\",INT=300,VAL=0"
"dpc1:CAT=\"ISUP: XMIT ACM TOT\",INT=1800,VAL=0"
"dpc1:CAT=\"ISUP: XMIT UBA TOT\",INT=300,VAL=0"
"dpc1:CAT=\"ISUP: XMIT UBA TOT\",INT=1800,VAL=0"
"dpc1:CAT=\"ISUP: XMIT MSG TOT\",INT=300,VAL=0"
"dpc1:CAT=\"ISUP: XMIT MSG TOT\",INT=1800,VAL=0"
"dpc1:CAT=\"ISUP: XMIT CCR TOT\",INT=300,VAL=0"
"dpc1:CAT=\"ISUP: XMIT CCR TOT\",INT=1800,VAL=0"
"dpc1:CAT=\"ISUP: RCV UBA TOT\",INT=300,VAL=0"
"dpc1:CAT=\"ISUP: RCV UBA TOT\",INT=1800,VAL=0"
"dpc1:CAT=\"ISUP: RCV MSG TOT\",INT=300,VAL=0"
"dpc1:CAT=\"ISUP: RCV MSG TOT\",INT=1800,VAL=0"
"dpc1:CAT=\"ISUP: UNEX MSG TOT\",INT=300,VAL=0"
"dpc1:CAT=\"ISUP: UNEX MSG TOT\",INT=1800,VAL=0"
"dpc1:CAT=\"ISUP: XMIT IAM TOT\",INT=300,VAL=0"
"dpc1:CAT=\"ISUP: XMIT IAM TOT\",INT=1800,VAL=0"
"dpc1:CAT=\"ISUP: UNREC MSG TOT\",INT=300,VAL=0"
"dpc1:CAT=\"ISUP: UNREC MSG TOT\",INT=1800,VAL=0"
"dpc1:CAT=\"ISUP: RCV IAM TOT\",INT=300,VAL=0"
"dpc1:CAT=\"ISUP: RCV IAM TOT\",INT=1800,VAL=0"
"dpc1:CAT=\"ISUP: RCV CFN TOT\",INT=300,VAL=0"
"dpc1:CAT=\"ISUP: RCV CFN TOT\",INT=1800,VAL=0"
"dpc1:CAT=\"ISUP: RCV CCR TOT\",INT=300,VAL=0"
"dpc1:CAT=\"ISUP: RCV CCR TOT\",INT=1800,VAL=0"
"dpc1:CAT=\"ISUP: XMIT ANM TOT\",INT=300,VAL=0"
"dpc1:CAT=\"ISUP: XMIT ANM TOT\",INT=1800,VAL=0"
"dpc1:CAT=\"ISUP: XMIT COT TOT\",INT=300,VAL=0"
"dpc1:CAT=\"ISUP: XMIT COT TOT\",INT=1800,VAL=0"
"dpc1:CAT=\"ISUP: RCV ANM TOT\",INT=300,VAL=0"
"dpc1:CAT=\"ISUP: RCV ANM TOT\",INT=1800,VAL=0"
"dpc1:CAT=\"ISUP: RCV INR TOT\",INT=300,VAL=0"
"dpc1:CAT=\"ISUP: RCV INR TOT\",INT=1800,VAL=0"
"dpc1:CAT=\"ISUP: RCV COT TOT\",INT=300,VAL=0"
"dpc1:CAT=\"ISUP: RCV COT TOT\",INT=1800,VAL=0"
"dpc1:CAT=\"ISUP: XMIT BLO TOT\",INT=300,VAL=0"
"dpc1:CAT=\"ISUP: XMIT BLO TOT\",INT=1800,VAL=0"
"dpc1:CAT=\"ISUP: ABN REL TOT\",INT=300,VAL=0"
"dpc1:CAT=\"ISUP: ABN REL TOT\",INT=1800,VAL=0"
"dpc1:CAT=\"ISUP: XMIT REL TOT\",INT=300,VAL=0"
"dpc1:CAT=\"ISUP: XMIT REL TOT\",INT=1800,VAL=0"
"dpc1:CAT=\"ISUP: RCV CVR TOT\",INT=300,VAL=0"
"dpc1:CAT=\"ISUP: RCV CVR TOT\",INT=1800,VAL=0"
"dpc1:CAT=\"ISUP: RCV CGU TOT\",INT=300,VAL=0"
"dpc1:CAT=\"ISUP: RCV CGU TOT\",INT=1800,VAL=0"
"dpc1:CAT=\"ISUP: XMIT SUS TOT\",INT=300,VAL=0"
"dpc1:CAT=\"ISUP: XMIT SUS TOT\",INT=1800,VAL=0"
"dpc1:CAT=\"ISUP: XMIT CVT TOT\",INT=300,VAL=0"
"dpc1:CAT=\"ISUP: XMIT CVT TOT\",INT=1800,VAL=0"
"dpc1:CAT=\"ISUP: XMIT GRA TOT\",INT=300,VAL=0"
"dpc1:CAT=\"ISUP: XMIT GRA TOT\",INT=1800,VAL=0"
"dpc1:CAT=\"ISUP: RCV SUS TOT\",INT=300,VAL=0"
"dpc1:CAT=\"ISUP: RCV SUS TOT\",INT=1800,VAL=0"
"dpc1:CAT=\"ISUP: RCV FOT TOT\",INT=300,VAL=0"
"dpc1:CAT=\"ISUP: RCV FOT TOT\",INT=1800,VAL=0"
"dpc1:CAT=\"ISUP: RCV GRS TOT\",INT=300,VAL=0"
"dpc1:CAT=\"ISUP: RCV GRS TOT\",INT=1800,VAL=0"

```

```

"dpc1:CAT=\"ISUP: XMIT CFN TOT\",INT=300,VAL=0"
"dpc1:CAT=\"ISUP: XMIT CFN TOT\",INT=1800,VAL=0"
"dpc1:CAT=\"ISUP: XMIT UBL TOT\",INT=300,VAL=0"
"dpc1:CAT=\"ISUP: XMIT UBL TOT\",INT=1800,VAL=0"
"dpc1:CAT=\"ISUP: RCV CVT TOT\",INT=300,VAL=0"
"dpc1:CAT=\"ISUP: RCV CVT TOT\",INT=1800,VAL=0"
"dpc1:CAT=\"ISUP: XMIT LPA TOT\",INT=300,VAL=0"
"dpc1:CAT=\"ISUP: XMIT LPA TOT\",INT=1800,VAL=0"
"dpc1:CAT=\"ISUP: XMIT FAC TOT\",INT=300,VAL=0"
"dpc1:CAT=\"ISUP: XMIT FAC TOT\",INT=1800,VAL=0"
"dpc1:CAT=\"ISUP: RCV FAC TOT\",INT=300,VAL=0"
"dpc1:CAT=\"ISUP: RCV FAC TOT\",INT=1800,VAL=0"
"dpc1:CAT=\"ISUP: RCV CGUA TOT\",INT=300,VAL=0"
"dpc1:CAT=\"ISUP: RCV CGUA TOT\",INT=1800,VAL=0"
"dpc1:CAT=\"ISUP: RCV UBL TOT\",INT=300,VAL=0"
"dpc1:CAT=\"ISUP: RCV UBL TOT\",INT=1800,VAL=0"
"dpc1:CAT=\"ISUP: XMIT USR TOT\",INT=300,VAL=0"
"dpc1:CAT=\"ISUP: XMIT USR TOT\",INT=1800,VAL=0"
"dpc1:CAT=\"ISUP: XMIT CGUA TOT\",INT=300,VAL=0"
"dpc1:CAT=\"ISUP: XMIT CGUA TOT\",INT=1800,VAL=0"
"dpc1:CAT=\"ISUP: RCV USR TOT\",INT=300,VAL=0"
"dpc1:CAT=\"ISUP: RCV USR TOT\",INT=1800,VAL=0"
"dpc1:CAT=\"ISUP: RCV ACM TOT\",INT=300,VAL=0"
"dpc1:CAT=\"ISUP: RCV ACM TOT\",INT=1800,VAL=0"
"dpc1:CAT=\"ISUP: XMIT FOT TOT\",INT=300,VAL=0"
"dpc1:CAT=\"ISUP: XMIT FOT TOT\",INT=1800,VAL=0"
"dpc1:CAT=\"ISUP: XMIT PAM TOT\",INT=300,VAL=0"
"dpc1:CAT=\"ISUP: XMIT PAM TOT\",INT=1800,VAL=0"
"dpc1:CAT=\"ISUP: RCV CGB TOT\",INT=300,VAL=0"
"dpc1:CAT=\"ISUP: RCV CGB TOT\",INT=1800,VAL=0"
"dpc1:CAT=\"ISUP: RCV RLC TOT\",INT=300,VAL=0"
"dpc1:CAT=\"ISUP: RCV RLC TOT\",INT=1800,VAL=0"
"dpc1:CAT=\"ISUP: RCV REL TOT\",INT=300,VAL=0"
"dpc1:CAT=\"ISUP: RCV REL TOT\",INT=1800,VAL=0"
"dpc1:CAT=\"ISUP: RCV CRM TOT\",INT=300,VAL=0"
"dpc1:CAT=\"ISUP: RCV CRM TOT\",INT=1800,VAL=0"
"dpc1:CAT=\"ISUP: XMIT CGBA TOT\",INT=300,VAL=0"
"dpc1:CAT=\"ISUP: XMIT CGBA TOT\",INT=1800,VAL=0"
"dpc1:CAT=\"ISUP: XMIT RLC TOT\",INT=300,VAL=0"
"dpc1:CAT=\"ISUP: XMIT RLC TOT\",INT=1800,VAL=0"
"dpc1:CAT=\"C7SP: SP DUR UNAVAIL\",INT=300,VAL=0"
"dpc1:CAT=\"C7SP: SP DUR UNAVAIL\",INT=1800,VAL=0"
"dpc1:CAT=\"ISUP: XMIT CRM TOT\",INT=300,VAL=0"
"dpc1:CAT=\"ISUP: XMIT CRM TOT\",INT=1800,VAL=0"
"dpc1:CAT=\"ISUP: RCV UCIC TOT\",INT=300,VAL=0"
"dpc1:CAT=\"ISUP: RCV UCIC TOT\",INT=1800,VAL=0"
"dpc1:CAT=\"ISUP: RCV CGBA TOT\",INT=300,VAL=0"
"dpc1:CAT=\"ISUP: RCV CGBA TOT\",INT=1800,VAL=0"
"dpc1:CAT=\"C7SP: XMIT MSU DROP/RTE\",INT=1800,VAL=0"
"dpc1:CAT=\"ISUP: XMIT GRS TOT\",INT=300,VAL=0"
"dpc1:CAT=\"ISUP: XMIT GRS TOT\",INT=1800,VAL=0"
"dpc1:CAT=\"ISUP: RCV RSC TOT\",INT=300,VAL=0"
"dpc1:CAT=\"ISUP: RCV RSC TOT\",INT=1800,VAL=0"
"dpc1:CAT=\"ISUP: XMIT RES TOT\",INT=300,VAL=0"
"dpc1:CAT=\"ISUP: XMIT RES TOT\",INT=1800,VAL=0"
"dpc1:CAT=\"ISUP: XMIT UCIC TOT\",INT=300,VAL=0"
"dpc1:CAT=\"ISUP: XMIT UCIC TOT\",INT=1800,VAL=0"
"dpc1:CAT=\"ISUP: RCV RES TOT\",INT=300,VAL=0"
"dpc1:CAT=\"ISUP: RCV RES TOT\",INT=1800,VAL=0"
"dpc1:CAT=\"ISUP: RCV PAM TOT\",INT=300,VAL=0"
"dpc1:CAT=\"ISUP: RCV PAM TOT\",INT=1800,VAL=0"
"dpc1:CAT=\"ISUP: RCV GRA TOT\",INT=300,VAL=0"
"dpc1:CAT=\"ISUP: RCV GRA TOT\",INT=1800,VAL=0"
"dpc1:CAT=\"ISUP: XMIT EXM TOT\",INT=300,VAL=0"

```

```

"dpc1:CAT=\"ISUP: XMIT EXM TOT\",INT=1800,VAL=0"
"dpc1:CAT=\"ISUP: XMIT CGU TOT\",INT=300,VAL=0"
"dpc1:CAT=\"ISUP: XMIT CGU TOT\",INT=1800,VAL=0"
"dpc1:CAT=\"ISUP: RCV EXM TOT\",INT=300,VAL=0"
"dpc1:CAT=\"ISUP: RCV EXM TOT\",INT=1800,VAL=0"
"dpc1:CAT=\"ISUP: XMIT INF TOT\",INT=300,VAL=0"
"dpc1:CAT=\"ISUP: XMIT INF TOT\",INT=1800,VAL=0"
"dpc1:CAT=\"ISUP: XMIT CQM TOT\",INT=300,VAL=0"
"dpc1:CAT=\"ISUP: XMIT CQM TOT\",INT=1800,VAL=0"
"dpc1:CAT=\"ISUP: RCV INF TOT\",INT=300,VAL=0"
"dpc1:CAT=\"ISUP: RCV INF TOT\",INT=1800,VAL=0"
"dpc1:CAT=\"SP: cInit in\",INT=900,VAL=0"
"dpc1:CAT=\"SP: cInit in\",INT=3600,VAL=0"
"dpc1:CAT=\"SP: cInit in\",INT=86400,VAL=5"
"dpc1:CAT=\"ISUP: RCV BLO TOT\",INT=300,VAL=0"
"dpc1:CAT=\"ISUP: RCV BLO TOT\",INT=1800,VAL=0"
"dpc1:CAT=\"ISUP: XMIT CPG TOT\",INT=300,VAL=0"
"dpc1:CAT=\"ISUP: XMIT CPG TOT\",INT=1800,VAL=0"
"dpc1:CAT=\"SP: PDU out\",INT=900,VAL=0"
"dpc1:CAT=\"SP: PDU out\",INT=3600,VAL=0"
"dpc1:CAT=\"SP: PDU out\",INT=86400,VAL=19"
"dpc1:CAT=\"ISUP: RCV CQR TOT\",INT=300,VAL=0"
"dpc1:CAT=\"ISUP: RCV CQR TOT\",INT=1800,VAL=0"
"dpc1:CAT=\"ISUP: XMIT CRA TOT\",INT=300,VAL=0"
"dpc1:CAT=\"ISUP: XMIT CRA TOT\",INT=1800,VAL=0"
"dpc1:CAT=\"ISUP: RCV CPG TOT\",INT=300,VAL=0"
"dpc1:CAT=\"ISUP: RCV CPG TOT\",INT=1800,VAL=0"
"dpc1:CAT=\"ISUP: XMIT INR TOT\",INT=300,VAL=0"
"dpc1:CAT=\"ISUP: XMIT INR TOT\",INT=1800,VAL=0"
"dpc1:CAT=\"ISUP: RCV CRA TOT\",INT=300,VAL=0"
"dpc1:CAT=\"ISUP: RCV CRA TOT\",INT=1800,VAL=0"

```

Using the Cisco MGC Viewer Toolkit

This section describes the various components of the Cisco MGC viewer toolkit. The Cisco MGC viewer toolkit is used to view different types of files on the Cisco MGC. This section describes the various components and the toolkit concept as a whole.

The Cisco MGC viewer toolkit is a suite of viewing tools that were developed to run on the Cisco MGC to provide quick and efficient access to diagnostic and troubleshooting information.

The following viewers are discussed in the following subsections:

- Launching the Cisco MGC Toolbar, page 3-103
- Using the Alarm and Measurement Viewer, page 3-103
- Using the Call Detail Record Viewer, page 3-107
- Using the Config-Lib Viewer, page 3-113
- Using the Log Viewer, page 3-114
- Using the Trace Viewer, page 3-117
- Using the Translation Verification Viewer, page 3-118
- Using the File Options Viewer, page 3-124
- Using the MGC Backup Viewer, page 3-125
- Using the MGC Restore Viewer, page 3-125

The Cisco MGC toolbar (Figure 3-1) is a graphical user interface (GUI) application used to launch the various viewers in the toolkit. Each application runs independently of the others, and there is a button for launching each application in the toolbar.

Figure 3-1 Cisco MGC Toolbar Window



You can run multiple instances of the Cisco MGC toolbar at one time, but only one instance of each tool can be running at a time, and different tools can be run simultaneously. If the selected application is already running, a message is displayed stating that your user ID and the application are already running. There is also a **Close** button on the toolbar, which is used to close the toolbar; however, closing the toolbar does not stop toolkit applications that are already running.



Caution

The potential exists for foreground (text) and background (non-text) settings to conflict because your local display settings might conflict with the toolkit's color settings, thus rendering the text within various fields in the toolkit applications unreadable.

If you have problems reading text on any of the toolkit screens, please change the foreground color to a darker color on your display to see if that solves the problem.

Launching the Cisco MGC Toolbar

To launch the Cisco MGC toolbar, complete the following steps:

- Step 1** Log in to the server on which you have installed the Cisco MGC toolkit, and enter the following command:

```
cd /opt/CMM/bin
```

- Step 2** Enter the following command to launch the Cisco MGC toolbar:

```
./start.sh tool
```

The MGC Toolbar window is displayed.

Using the Alarm and Measurement Viewer

The alarm and measurement viewer helps you view and search records that reside in the alarm and measurement record logs. The formats of the various alarm and measurement records are specified in the *Cisco Media Gateway Controller Software Release 7 Messages Reference Guide*. These records are not designed for user reading, but for database loading. These viewers can help you understand these records, and they also provide useful searching functions based on the components and categories you select.

The alarm and measurement viewer offers a help file, which contains information about the viewer. To access the information, click the **Help** menu, select **ReadMe**, and the help text is displayed. You can also use this viewer to determine the current timestamp. To do this, click the **Time** menu, select **TimeStamp**. The current timestamp is displayed in a window.

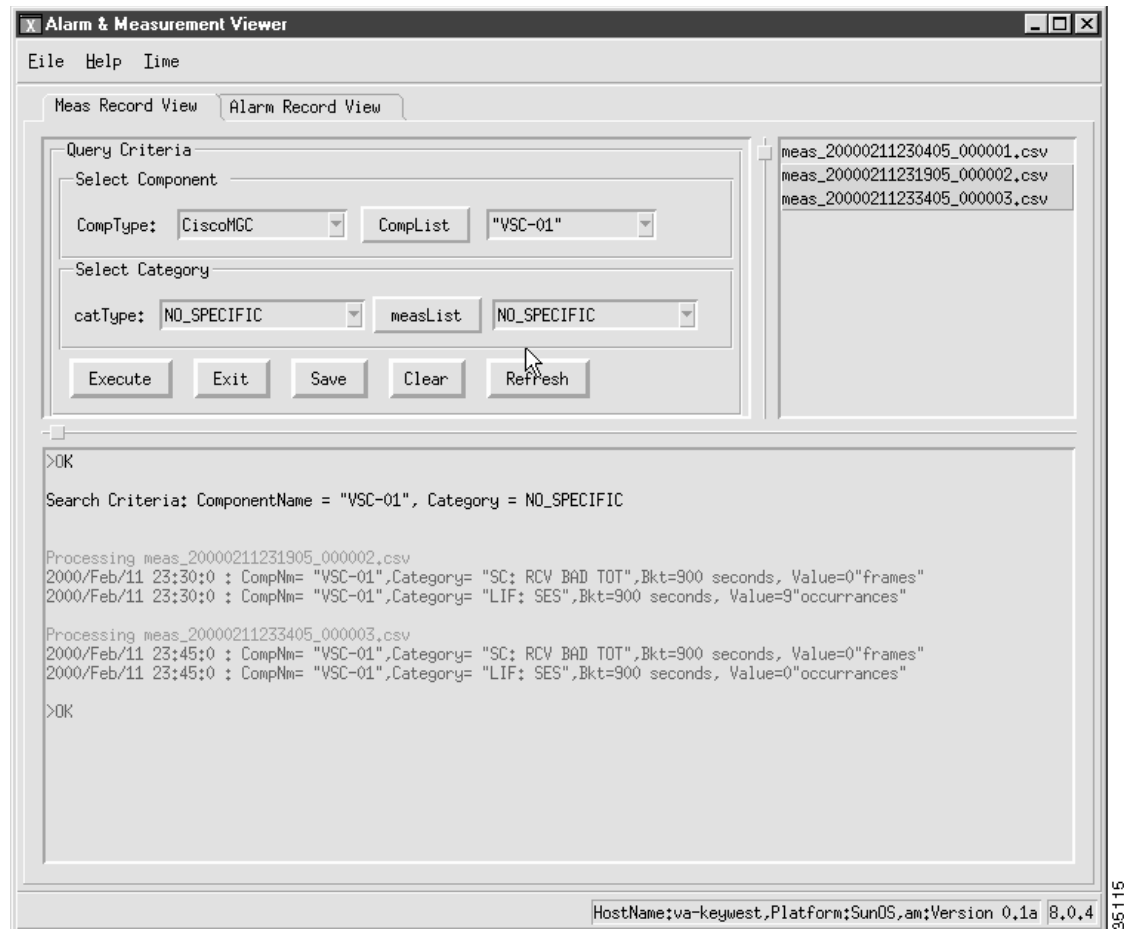
You can exit the Alarm and Measurement Viewer in one of two ways: in the Query Criteria portion of the window, click **Exit**, or from the **File** menu, select **Exit**.

Viewing and Searching System Measurement Files

Complete the following steps to view and search various system measurement files:

- Step 1** Open the alarm and measurement viewer. To do this, click **Alarm&Meas Viewer** on the Cisco MGC Toolbar. A popup window displays warning you that running this tool can impact system performance and asking you if you want to launch the tool. Click **Yes**. The Alarm & Measurement Viewer window loads and displays the Meas Record View tab window by default (Figure 3-2).
- Step 2** Select the system measurement file(s) you want to display from the field to the right of the Query Criteria portion of the window.

Figure 3-2 Meas Record View Tab Window



You can select multiple files in this field using any of the following techniques:

- Select a range of files by clicking a file, holding the mouse button down, dragging the mouse pointer down to the last file you would like to select, and letting go of the mouse button.
- Select a range of files by holding down the **Shift** key, clicking the first file in the range, clicking the last file in the range, and releasing the **Shift** key.

- Select multiple files not located next to each other by holding down on the **Ctrl** key and clicking each file you want to include.
- Step 3** To search by a component, select a component type from the **CompType** drop-down list box. If you do not want to search by a component or you want to view the entire content of the file(s), select the *NO_SPECIFIC* entry.
- Click **CompList** to acquire the configured components for the type you selected. The results are displayed in the drop-down list box next to the button. Select a component from that list box.
- Step 4** To search by a category, select a category type from the **catType** drop-down list box. If you do not want to search by a category or you want to view the entire content of the file(s), select the *NO_SPECIFIC* entry.
- Click **measList** to acquire the configured categories for the type you selected. The results are displayed in the drop-down list box next to the button. Select a category from that list box.
- Step 5** Click **Execute** to search the selected system measurement file(s). The results of the search are displayed as blue text in the field at the bottom of the window.
- Step 6** If you want to perform additional searches, repeat steps 2 to 5. The color of the text from the old search changes from blue to black and the newly requested search data is inserted as blue text, appearing after the old data. Scroll down through the field to view the data you have added (You can clear the display field by clicking **Clear** before you click **Execute**, if you no longer require the previously requested data).
- Step 7** If you want to save the displayed data, click **Save**. The contents of the field are saved to a file with the following directory path:
- `$BASEDIR/etc/cust_specific/toolkit/measRec.log`
- If you perform another search and save the resulting content, the contents of the field are added into the *measRec.log* file, after the previously saved data. If you do not want the data to be added onto the previous data, you must change the name of the *measRec.log* file before you save again. To change the name of a file, refer to the procedures in the “Using the File Options Viewer” section on page 3-124.
- If you do not find your desired data, you can update the list of system measurement files by clicking **Refresh**. Repeat the above steps to search through the newest files.

Viewing and Searching Alarm Record Files

Complete the following steps to view and search various system alarm files:

- Step 1** Open the alarm and measurement viewer. To do this, click **Alarm&Meas Viewer** on the Cisco MGC Toolbar. A popup window displays warning you that running this tool can impact system performance and asking you if you want to launch the tool. Click **Yes**. The Alarm & Measurement Viewer window loads and displays.
- Step 2** Click the **Alarm Record View** tab. The Alarm Record View tab window displays (Figure 3-3).
- Step 3** Select the alarm file(s) you want to display from the field to the right of the Query Criteria portion of the window.

You can select multiple files in this field using any of the following techniques:

- Select a range of files by clicking a file, holding the mouse button down, dragging the mouse pointer down to the last file you would like to select, and letting go of the mouse button.
- Select a range of files by holding down the **Shift** key, clicking the first file in the range, clicking the last file in the range, and releasing the **Shift** key.

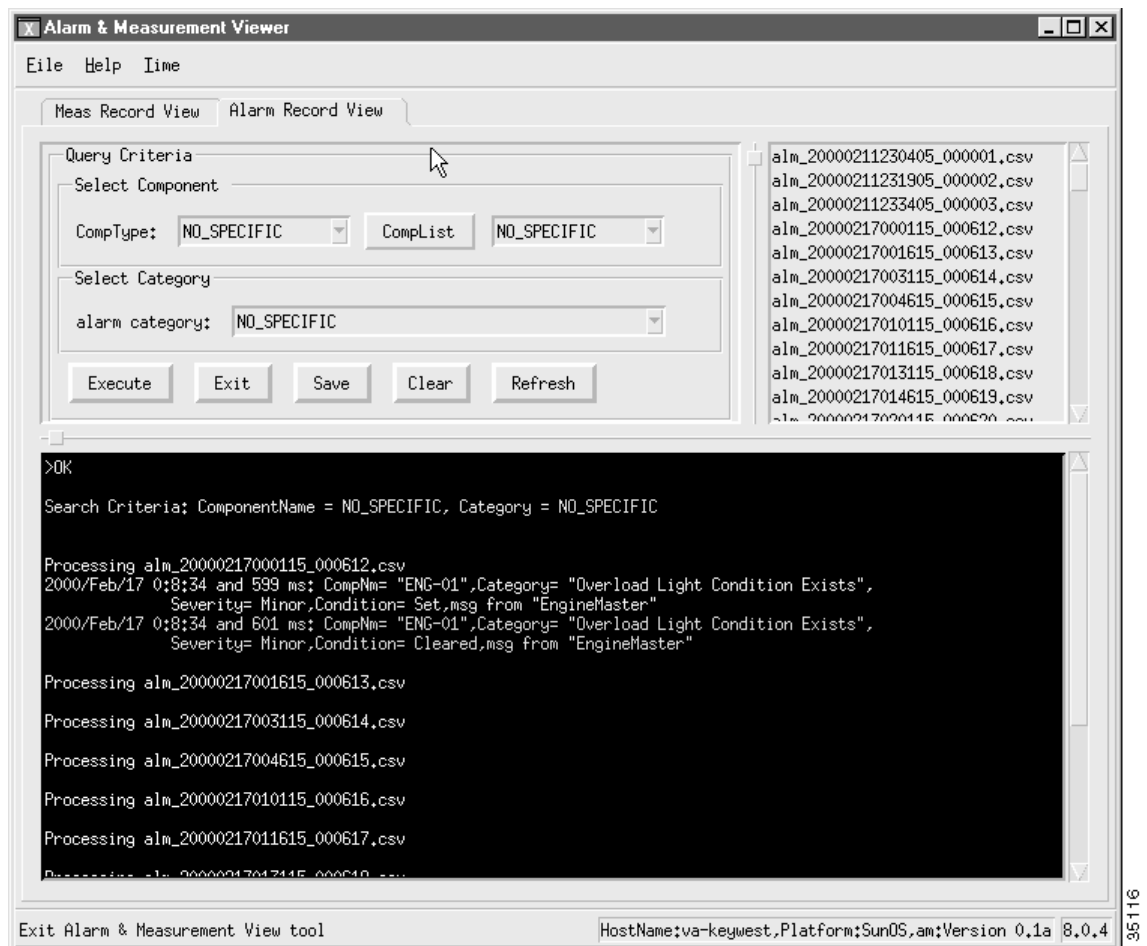
- Select multiple files not located next to each other by holding down on the **Ctrl** key and clicking each file you want to include.

Step 4 To search by a component, select a component type from the CompType drop-down list box. If you do not want to search by a component or you want to view the entire contents of the file(s), select the *NO_SPECIFIC* entry.

Click **CompList** to acquire the configured components for the type you selected. The results are displayed in the drop-down list box next to the button. Select a component from that list box.

Step 5 To search by a category, select a category type from the alarm category drop-down list box. If you do not want to search by a category or you want to view the entire contents of the file(s), select the *NO_SPECIFIC* entry.

Figure 3-3 Alarm Record View Tab Window



Step 6 Click **Execute** to display the contents of the selected alarm file(s). The contents are displayed as multicolored text in the field at the bottom of the window.

The following list describes the text colors associated with the alarm types

- Comments—white
- Cleared—green
- Information—blue

- Minor—yellow
- Major—orange
- Critical—red

Step 7 If you want to perform additional searches, repeat steps 2 to 6. The color of the text from the old search changes from multicolored to blue and the newly requested search data is inserted as multicolored text, appearing after the old data. Scroll down through the field to view the data you have added. You can clear the display field by clicking **Clear** before you click **Execute**, if you no longer require the previously requested data.

Step 8 If you want to save the displayed data, click **Save**. The contents of the field are saved to a file with the following directory path:

\$BASEDIR/etc/cust_specific/toolkit/alarmRec.log

If you perform another search and save that content again, the contents of the field are added into the alarmRec.log file, after the previously saved data. If you do not want the data to be added onto the previous data, you must change the name of the alarmRec.log file before you save again. To change the name of a file, refer to the procedures in the “Using the File Options Viewer” section on page 3-124.

If you do not find your desired data, you can update the list of alarm files by clicking **Refresh**. Repeat the above steps to search through the newest files.

Using the Call Detail Record Viewer

CDRs contain basic call billing information, such as date and time, duration, and the calling number and called number. CDR records are written into files that contain information about telephone activity. CDR files are saved in a comma-delimited format (called a “Tag-Length-Value” or TLV file). The TLV file is a generic format that can be easily imported into most third-party mediation applications.

The CDR dumper (see Figure 1-1) provides logging capabilities on the Cisco MGC for all CDRs. Also, the CDR dumper supports external user application programming interfaces (APIs). The APIs allow users to get a real-time feed of CDRs and call detail blocks (CDBs) from the Cisco MGC that can be routed to a third-party mediation application for use in billing.

The CDR dumper operates according to the configuration set up in the XECfgParm file. When certain thresholds are met, the CDR dumper closes and saves the generated CDB records into the \$BASEDIR/var/spool directory. It then passes the filename and fork to the TLV converter application.

The CDR viewer is designed to help you view and search call detail records that reside in the CDR logs. The formats of the CDBs and call data elements (CDEs) that comprise CDRs are specified in the *Cisco Media Gateway Controller Software Release 7 Billing Interface Guide*. These records are designed for database loading, not user reading. The CDR Viewer can help you understand these records, and it also provides useful searching functions based on the search criteria you select.



Note

Your screen might be slightly different from this example, depending on which release of the software you are running.

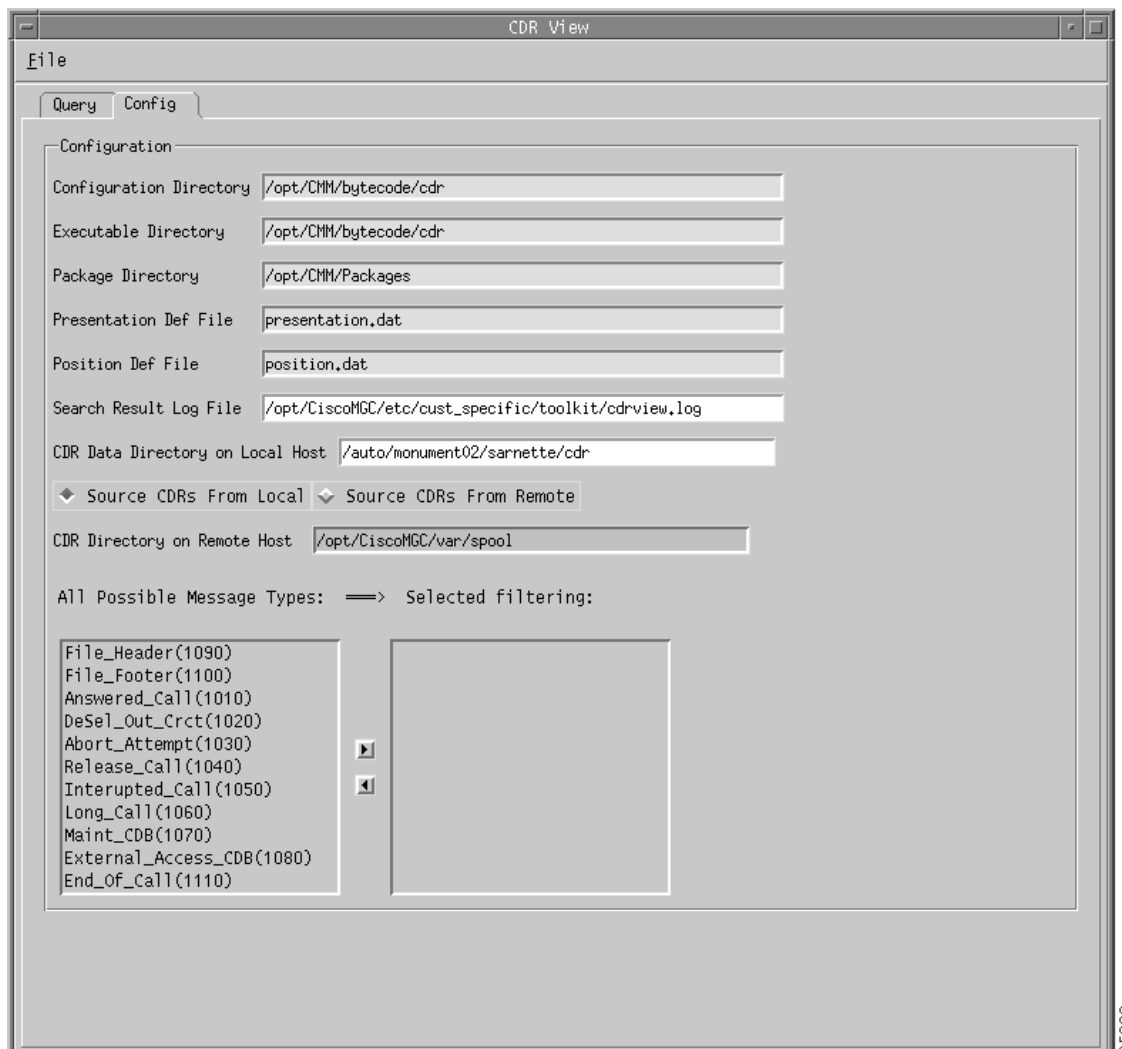
You can exit the CDR viewer in one of two ways: in the **Query Criteria** portion of the window, click **Exit**, or from the **File** menu, select **Exit**.

Configuring the CDR Viewer

Whenever you start the CDR viewer, you must select several configuration settings before you can view or search the CDR files. To do this, complete the following steps.

- Step 1** Open the CDR viewer. To do this, click **CDR Viewer** on the Cisco MGC Toolbar. A popup window displays warning you that running this tool can impact system performance and asking you if you want to launch the tool. Click **Yes**. The CDR Viewer window loads and displays.
- Step 2** Click the **Config** tab. The Config tab window displays (Figure 3-4).
The first five fields in the window cannot be modified. These fields list the directory paths and file names for the related data files.
- Step 3** You can modify the directory path and file name for the file in which any CDR search results can be saved. To do this, click in the Search Result Log File field and change the displayed information.

Figure 3-4 Config Tab Window



**Note**

We recommend that you not use this field to change the directory information for the CDR search results file.

Step 4

You can also set the source for your CDR information to either a local or remote host.

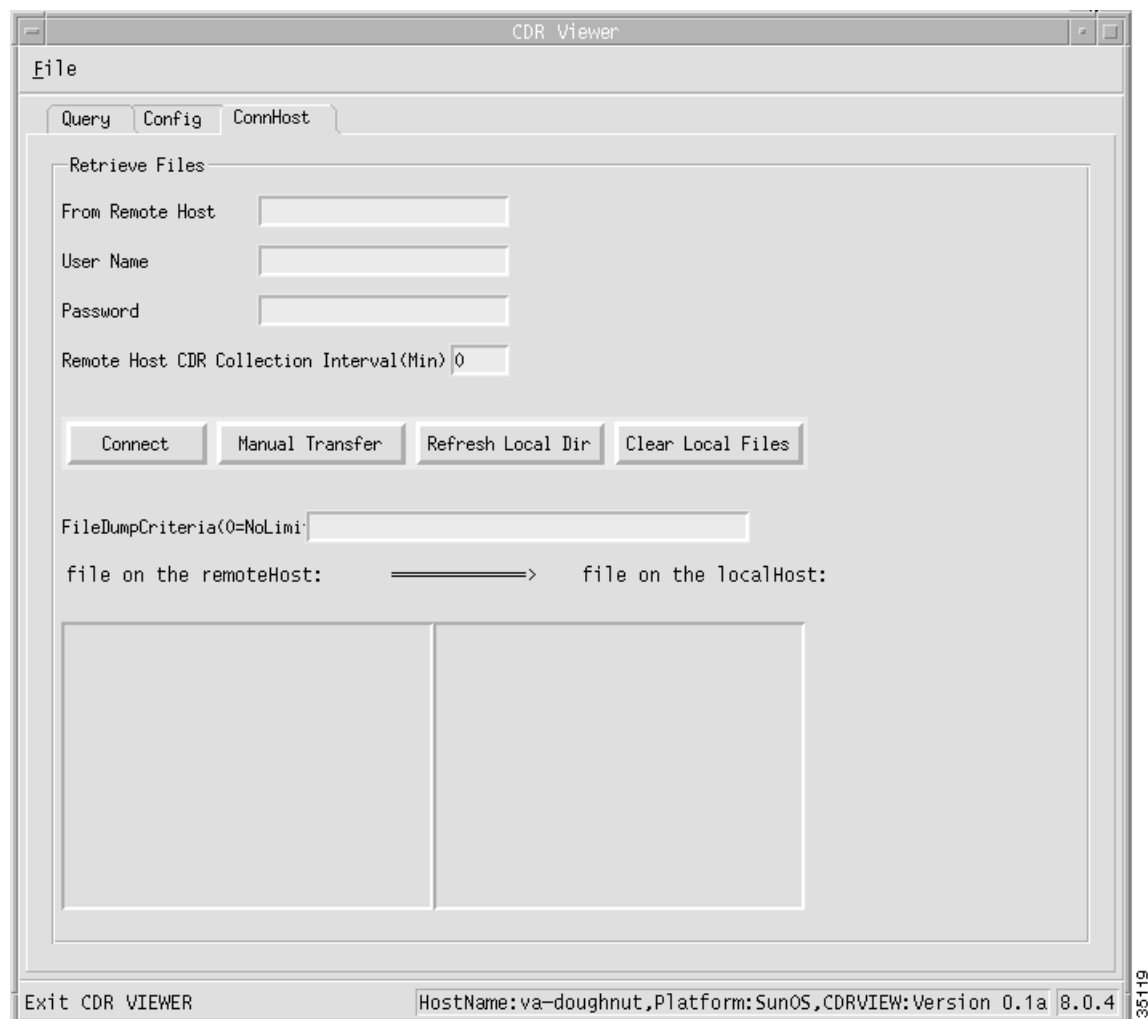
If you want to use a local host as your source for CDR information, click the **Source CDRs From Local** check box and proceed to Step 5.

If you want to use a remote host as your source for CDR information, click the **Source CDRs From Remote** check box and proceed to Step 6.

**Note**

If you change your CDR source from local to remote, the tab for the ConnHost window (Figure 3-5) appears. If you change your CDR source from remote to local, the tab for the ConnHost window disappears.

Figure 3-5 ConnHost Tab Window



- Step 5** You can modify the CDR source directory on your local host. To do this, click in the CDR Data Dictionary on Local Host field and change the displayed information.
- Proceed to Step 11 to select the message type(s) for which you are searching.
- Step 6** You can modify the CDR source directory on your remote host. To do this, click in the CDR Directory on Remote Host field and change the displayed information.
- Step 7** Click the **ConnHost** tab to display the ConnHost tab window (Figure 3-5).
- Step 8** You can add or modify the name of the remote host. To do this, select the From Remote Host field and enter the name of the remote host you want to use a source for your CDR files.
- Step 9** If you add or modify a remote host name, you must enter user account information for the viewer to use in accessing the host. To do this, enter the appropriate user name and password data in the User Name and Password fields, respectively.
- Step 10** You can modify how frequently the CDR viewer checks the remote host for new CDB files. To do this, enter the value you want (in minutes) in the Remote Host CDR Collection Interval(Min) field.
- If you set the interval value above zero, after you click **Connect**, you are notified by a popup message box when new CDB files are deposited on the remote host. You can click **OK** in the message box to dynamically update the CDB files on the local host, or you can click **NO** to keep the local CDB file directory as it is.
- If you set the interval value to zero, you are not notified of file changes on the remote host, and the CDB files on the local host are not dynamically updated.
- The FileDumpCriteria(0=NoLimit) field displays the configuration information for CDRs on the Cisco MGC. This content of this field cannot be modified.
- Step 11** You must specify the message type(s) for which you are searching. To do this, click the **Config** tab to display the Config tab window (Figure 3-4), and select the message type(s) you are looking for in the All Possible Message Types field. Click the right arrow button and the specified message type(s) are displayed in the Selected filtering field.
- You can select multiple files in this field using any of the following techniques:
- Select a range of files by clicking a file, holding the mouse button down, dragging the mouse pointer down to the last file you would like to select, and letting go of the mouse button.
 - Select a range of files by holding down the **Shift** key, clicking the first file in the range, clicking the last file in the range, and releasing the **Shift** key.
 - Select multiple files not located next to each other by holding down on the **Ctrl** key and clicking each file you want to include.
- You can remove message type(s) from your search criteria by selecting the desired message type(s) in the Selected filtering field and clicking the left arrow button.

Searching the CDR Files

You can search through the various alarm files by component and category. To do this, complete the following steps:

- Step 1** Open the CDR viewer. To do this, click **CDR Viewer** on the Cisco MGC toolbar. A popup window displays warning you that running this tool can impact system performance and asking you if you want to launch the tool. Click **Yes**. The CDR Viewer window loads and displays the Query tab window by default (Figure 3-6).

If you have just opened the viewer, you must configure it before you can search the CDR files. Refer to “Configuring the CDR Viewer” section on page 3-108.

Step 2 If your CDR files are coming from a local host, proceed to Step 8.

If your CDR files are coming from a remote host, proceed to Step 3.

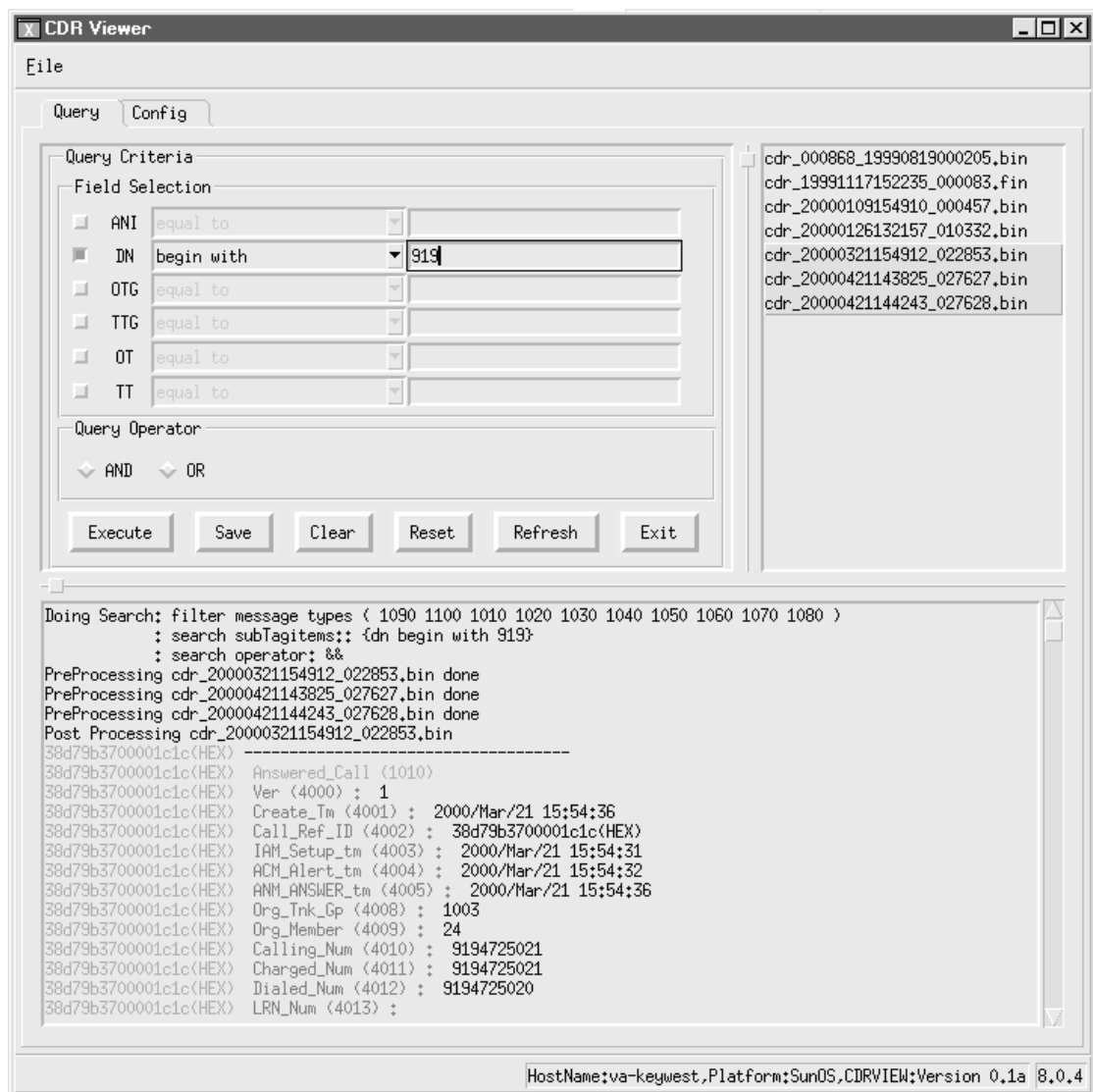
Step 3 Click the **ConnHost** tab to open the ConnHost tab window.

Step 4 If the fields in the window are properly data filled, click **Connect** to establish contact with the remote host.

If the fields in the window are not properly data filled, perform the configuration steps for this window as described in the “Configuring the CDR Viewer” section on page 3-108. Once you have completed this, resume this procedure.

Step 5 Select the file(s) you want to search from the file on the remoteHost field.

Figure 3-6 Query Tab Window



You can select multiple files in this field using any of the following techniques:

- Select a range of files by clicking a file, holding the mouse button down, dragging the mouse pointer down to the last file you would like to select, and letting go of the mouse button.
- Select a range of files by holding down the **Shift** key, clicking the first file in the range, clicking the last file in the range, and releasing the **Shift** key.
- Select multiple files not located next to each other by holding down on the **Ctrl** key and clicking each file you want to include.

Step 6 Click **Manual Transfer** to copy your selected file(s) to the local host.

If you want to remove the files from your local host, you can click **Clear Local Files**. If you want to update the listed files in the file on the localHost field, you can click **Refresh Local Dir**.

Step 7 Click the **Query** tab to display the Query tab window.

Step 8 Select the CDR file(s) you want to search from the field to the right of the Query Criteria portion of the window.

You can select multiple files in this field using any of the following techniques:

- Select a range of files by clicking a file, holding the mouse button down, dragging the mouse pointer down to the last file you would like to select, and letting go of the mouse button.
- Select a range of files by holding down the **Shift** key, clicking the first file in the range, clicking the last file in the range, and releasing the **Shift** key.
- Select multiple files not located next to each other by holding down on the **Ctrl** key and clicking each file you want to include.

Step 9 If you want to view your selected CDR file(s) in their entirety, proceed to Step 13.

If you want to search through your selected CDR file(s) for particular type(s) of CDRs, proceed to Step 10.

Step 10 You can search through your selected CDR files based on six different field values:

- ANI—Calling Party Number
- DN—Dialed Number
- OTG—Originating Trunk Group Number
- TTG—Terminating Trunk Group Number
- OT—Originating Trunk Number
- TT—Terminating Trunk Number

To select a field value, click the check box next to the name. You can select as few or as many field values as you require.

Step 11 Enter a search qualifier and related string for each of the field values you selected. To do this, choose a search qualifier, as defined below, for the search string from the drop-down list box to the right of a field value you have selected.

- Equal to—The selected field in the CDB is equal to the value defined in the search string.
- Has—Any substring of the selected field in the CDB has the value defined in the search string.
- Begins with—The selected field in the CDB begins with the value defined in the search string.
- Ends with—The selected field in the CDB ends with the value defined in the search string.

Enter a search string in the field to the right of the search qualifier you just choose.

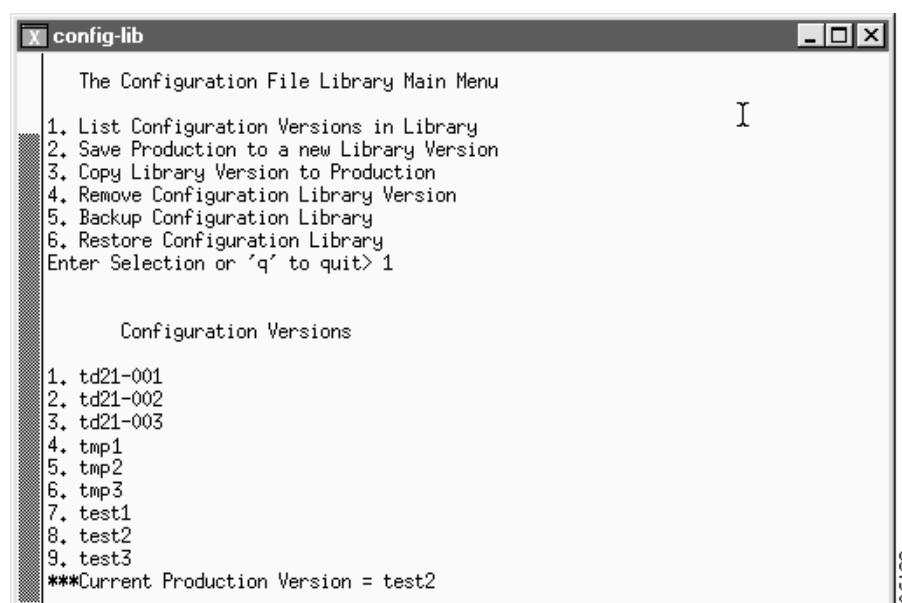
Repeat this step for all field values that you have selected for your search.

- Step 12** Choose a query operator (AND or OR) for your search. You can search for CDBs that have all of the field values you selected (AND) or you can search for CDBs that have any of the field values you selected (OR). The default value is AND. Click the appropriate check box to specify your query operator.
- Step 13** Click **Execute** to display the contents of the selected alarm file(s). A popup window displays while the contents load. The contents are displayed as multicolored text in the field at the bottom of the window.
- Step 14** If you want to perform additional searches, repeat steps 2 to 13. The color of the text from the old search changes from multicolored to black and the newly requested search data is inserted as multicolored text, appearing after the old data. Scroll down through the field to view the data you have added. You can clear the display field by clicking **Clear** before you click **Execute**, if you no longer require the previously requested data.
- Step 15** If you want to save the displayed data, click **Save**. The contents of the field are saved to the file you specified in the Config tab window.
- If you perform another search and save that content again, the contents of the field are added to the same file, after the previously saved data. If you do not want the data to be added to the previous data, you must change the name of the file before you save again. To change the name of a file, refer to the procedures in the “Using the File Options Viewer” section on page 3-124.
- Step 16** If you do not find your desired data, you can update the list of alarms files by clicking **Refresh**. Repeat the above steps to search through the newest files.

Using the Config-Lib Viewer

You can use the Config-Lib viewer (Figure 3-7) to manage the contents of the configuration library. The configuration library stores the various system configurations that you created while you provisioned your Cisco MGC.

Figure 3-7 Config-Lib Viewer Window



Click **CONFIG-LIB** on the Cisco MGC toolbar to open an xterm window and execute the config-lib script. To quit the Config-Lib Viewer, enter q at the prompt.

The Config-Lib Viewer enables you to do the following functions:

- **List Configuration Versions in Library**—Returns a listing of the configuration versions stored in the library and identifies the configuration that is currently being used (referred to as the production version). To activate this function, enter 1 at the prompt.
- **Save Production to a new Library Version**—Saves your current configuration settings to a new version file. When you select this function, the Cisco MGC software must not be running, or an error message is displayed. For more information on stopping the Cisco MGC software, refer to the “Shutting Down the Cisco MGC Software Manually” section on page 2-4. To activate this function, enter 2 at the prompt and then enter the name for the new library version.
- **Copy Library Version to Production**—Restores your Cisco MGC to the settings in an old configuration version. When you select this function, the Cisco MGC software must not be running, or an error message is displayed. For more information on stopping the Cisco MGC software, refer to the “Shutting Down the Cisco MGC Software Manually” section on page 2-4. To activate this function, enter 3 at the prompt and then enter the number of the library version to be set as the production version.

**Note**

We recommend that you not attempt to restore an old configuration version without the assistance of the Cisco TAC. Refer to the “Obtaining Technical Assistance” section on page xviii for more information about contacting the Cisco TAC.

- **Remove Configuration Library Version**—Deletes a configuration version from the library. When you select this function, the Cisco MGC software must not be running, or an error message is displayed. For more information on stopping the Cisco MGC software, refer to the “Shutting Down the Cisco MGC Software Manually” section on page 2-4. To activate this function, enter 4 at the prompt and then enter the number of the library version to be deleted.

**Caution**

If you are using a software version prior to 7.4(11), we recommend that you limit the number of configuration versions stored in the configuration library to 64, to prevent a possible failure when performing a switchover or using the **prov-sync** command. If you are storing more than 64 configuration versions, we recommend that you delete some of your configuration versions. If you are using software release 7.4(11) or higher, the disk monitor script automatically controls the number of versions stored in the configuration library. For more information, refer to the *Release Notes for the Cisco Media Gateway Controller Software*. For more information about the disk monitor script, refer to the “Automatic Disk Space Monitoring” section on page 3-24.

- **Backup Configuration Library**—Stores your current configuration library as a .tar file. As of Release 7.4(12), this option is no longer valid.
- **Restore Configuration Library**—Recreates the configuration library you stored previously as a .tar file. As of Release 7.4(12), this option is no longer valid.

Using the Log Viewer

The Log Viewer offers selection and reporting capabilities that allow you to retrieve and display log messages from the system log files.

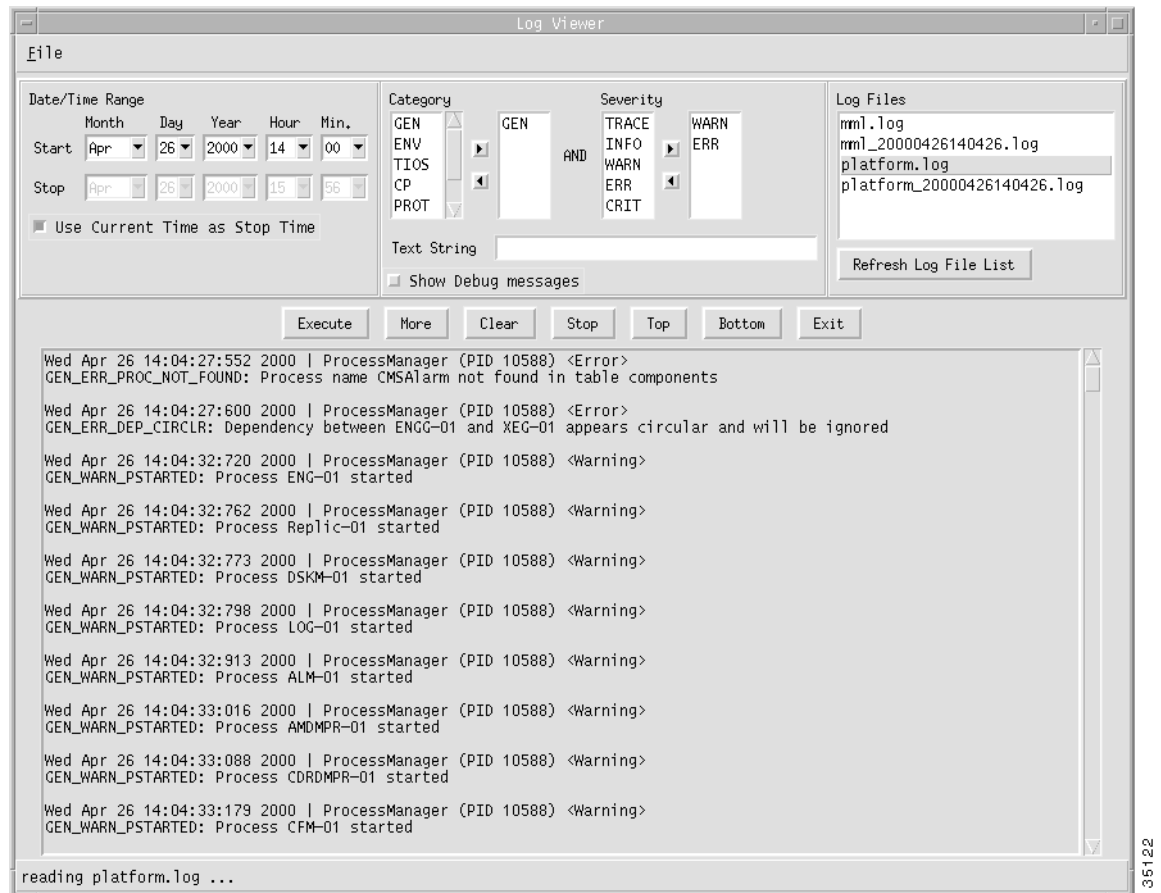
You can exit the Log Viewer in one of two ways: click **Exit**, or select **Exit** from the **File** menu.

Searching Log Record Files

Complete the following steps to search through various system log files:

- Step 1** Open the log viewer. To do this, click **Log Viewer** on the Cisco MGC Toolbar. A popup window displays warning you that running this tool can impact system performance and asking you if you want to launch the tool. Click **Yes**. The Log Viewer window loads and displays (Figure 3-8).

Figure 3-8 Log Viewer Window



- Step 2** Select the log file you want to display from the Log Files field.



Note

If the log file you want to view are not displayed in the Log Files field, refresh the list by clicking **Refresh Log File List**, or by clicking the **File** menu and selecting **Refresh**.

If the desired file is still not displayed, you might need to change the directory path used by the viewer. To do this, click the **File** menu and select **Log Directory**. Enter the appropriate directory path in the Log Directory field and click **Modify** to save the new settings. The log files contained in the directory path you specified are displayed in the Log Files field.

- Step 3** You can search for logs that occurred between a certain dates and times, specifying month, day, year, hour, and minute settings. To do this, select a starting date and time from the Start Date/Time drop-down list boxes and then select a stopping date and time from the Stop Date/Time drop-down list boxes.

The current date and time are the default values for both the start and stop values for the time period; however, using these values results in a null search (no records).

The **Use Current Time as Stop Time** check box, if selected, disables the Stop Date/Time drop-down list boxes and allows searching to continue to the end of the file.

- Step 4** You can search for logs of certain log categories. To do this, select your desired category or categories by clicking one or more entries in the Category list box. To select multiple entries, hold down either the **Ctrl** or **Shift** key while clicking.

The available categories are:

- GEN
- ENV
- TIOS
- CP
- PROT
- MGMT
- MML

Click the right arrow to enter your selected categories into the search. The selected categories appear in the list box to the right of the arrow buttons. To deselect a category, click one or more entries in the right list box and click the left arrow.

- Step 5** You can search for logs of certain severities. To do this, select a severity or severities by clicking one or more entries in the Severity list box. To select multiple entries, hold down either the **Ctrl** or **Shift** key while clicking.

The severity choices are cumulative—each level selected also displays all levels below it. For example, the ERR selection displays both ERR (error) and CRIT (critical) messages. The severity levels are

- TRACE
- INFO
- WARN
- ERR
- CRIT

Click the right arrow to enter your selected categories into the search. The selected categories appear in the list box to the right of the arrow buttons. To deselect a category, click one or more entries in the right list box and click the left arrow.

- Step 6** You can search for logs that contain a particular text string. To do this, enter the desired search string in the Text String field. The text is case-sensitive, and all characters are allowed.

- Step 7** You also can choose to display debug messages. Debug messages do not conform to the log message format. If you select this option, the debug messages are filtered only on date/time and text string. To do this, click the **Show Debug Messages** check box. Debug messages similar to the following are displayed:

```
platform.log ... : currently active log
```

```
Fri Apr 14 17:57:19:253 2000 | ProcessManager (PID 24929) <Debug>
initialized process info for 'POM-01'
```

```
Fri Apr 14 17:57:25:908 2000 | ProcessManager (PID 24929) <Debug>  
Received heartbeat response from process CFM-01
```

- Step 8** Click **Execute** to display the results from the selected alarm file(s). The results are displayed in the field at the bottom of the window, in 5-MB blocks.

While the application is searching through the log files, a dialog box appears. This dialog box displays the progression of the search. It also allows you to stop searching by pressing **Stop**.

Your results may be lengthy, resulting in several pages of information. You can use several buttons to navigate through your results. To go to the end of your results, click **Bottom**. To go to the next 5-MB page of results, click **More**. To go to the beginning of your results, click **Top**.

- Step 9** If you want to save the displayed data, click the **File** menu and select **Save**. A popup window lists the default save directory (/opt/CiscoMGC/etc/cust_specific/toolkit). Enter a file name for your data in the File Name field and click **Save** to save your data.

- Step 10** If you want to perform additional searches, repeat steps 2 to 9. The old search data is replaced by the new search data. You can clear the display field by clicking **Clear** before you click **Execute**.

Using the Trace Viewer

You can use the trace viewer as part of performing a call trace. Clicking **Trace Viewer** in the Cisco MGC toolbar opens the Traces Files window, which lists the call trace files from which you can choose (Figure 3-9). When you select a file, you can click **View**, which opens the Trace Viewer window (Figure 3-10), which allows you to perform a variety of call trace activities. For more information about call traces, refer to the “Tracing” section on page 8-102.

Figure 3-9 Trace Viewer Window

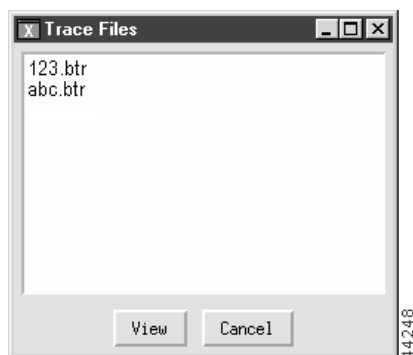
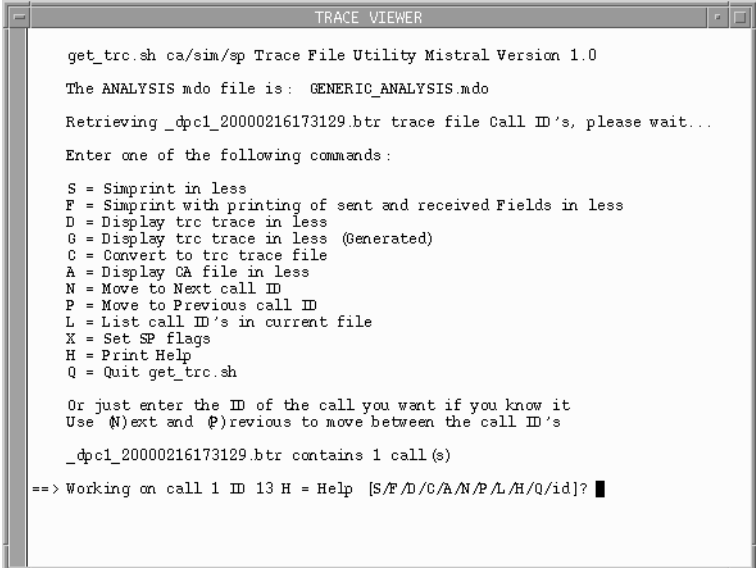


Figure 3-10 Trace Viewer Window


```

TRACE VIEWER

get_trc.sh ca/sim/sp Trace File Utility Mistral Version 1.0

The ANALYSIS mdo file is:  GENERIC_ANALYSIS.mdo

Retrieving _dpc1_20000216173129.btr trace file Call ID's, please wait...

Enter one of the following commands:

S = Simprint in less
F = Simprint with printing of sent and received Fields in less
D = Display trc trace in less
G = Display trc trace in less (Generated)
C = Convert to trc trace file
A = Display CA file in less
N = Move to Next call ID
P = Move to Previous call ID
L = List call ID's in current file
X = Set SP flags
H = Print Help
Q = Quit get_trc.sh

Or just enter the ID of the call you want if you know it
Use (N)ext and (P)revious to move between the call ID's

_dpc1_20000216173129.btr contains 1 call(s)

==> Working on call 1 ID 13 H = Help [S/F/D/C/A/N/P/L/H/Q/id]?

```

Using the Translation Verification Viewer

The translation verification viewer offers a means of interfacing with the translation verification tool. The translation verification tool provides you with a means to understand how calls are being processed based on your system's dial plan. This tool creates a simulation of a call being processed by your system's dial plan.



Note

The translation verification viewer does not simulate the screening database and cause analysis dial plan functions.

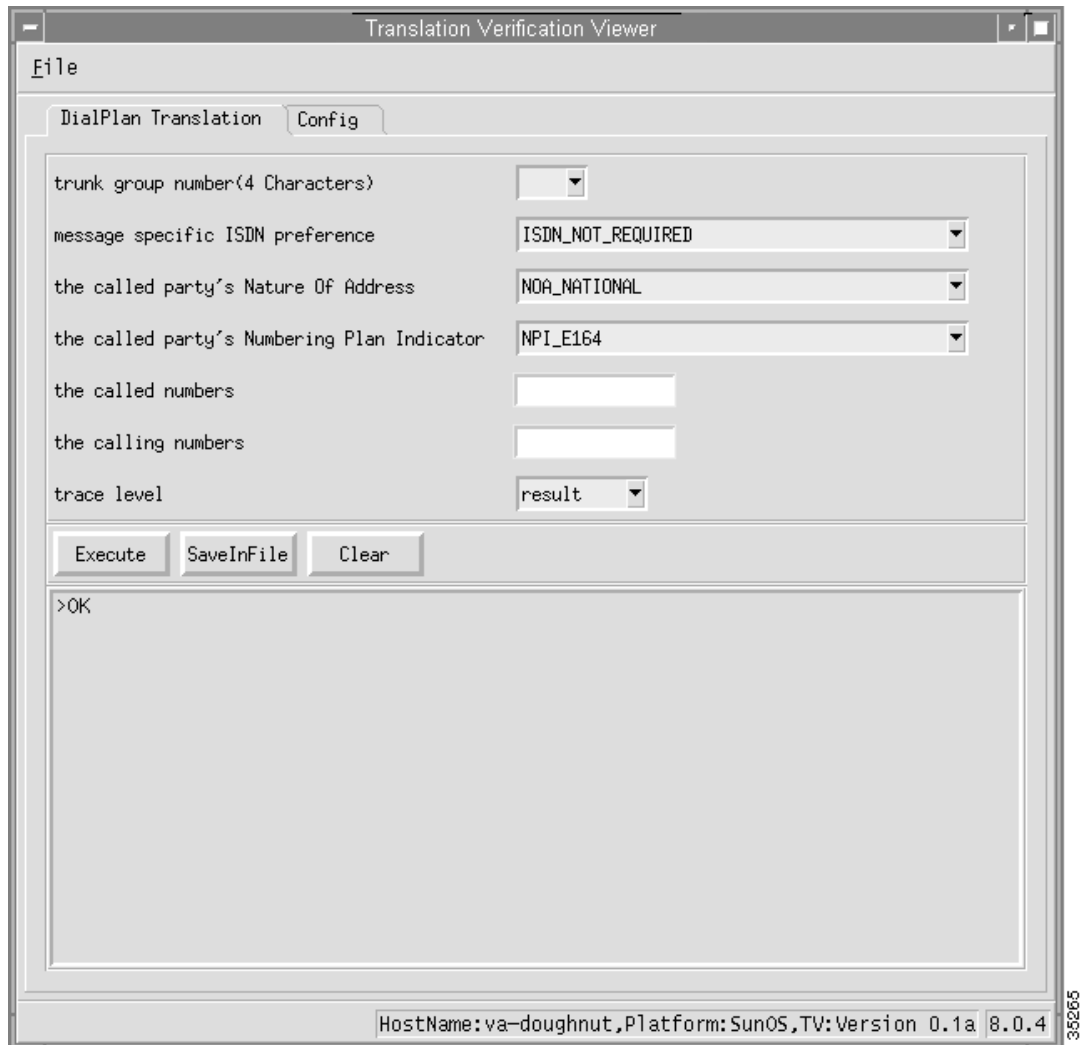
You can exit the translation verification viewer by clicking on the **File** menu and selecting **Exit**.

Verifying a Dial Plan Translation

Complete the following steps to verify a dial plan translation:

- Step 1** Open the translation verification viewer. To do this, click **Translation Verification** on the Cisco MGC toolbar. A popup window displays warning you that running this tool can impact system performance and asking you if you want to launch the tool. Click **Yes**. The Translation Verification Viewer window loads and the DialPlan Translation tab window is displayed by default (Figure 3-11).
- Step 2** Enter the incoming trunk group number for your simulated call in the trunk group number field.
- Step 3** Specify an ISDN preference for the selecting of the outgoing trunk by choosing a value from the message specific ISDN preference drop-down list box. The following values are valid for this field.
 - ISDN_NOT_REQUIRED (default value)
 - ISDN_PREFERRED
 - ISDN_REQUIRED

Figure 3-11 Dial Plan Translation Tab Window



Step 4 Specify the Nature Of Address (NOA) setting for the called party by selecting a value from the called party's Nature of Address drop-down list box. The following values are valid for this list.

- NOA_NATIONAL (default value)
- NOA_NONE
- NOA_UNKNOWN
- NOA_SUBSCRIBER
- NOA_INTERNATIONAL
- NOA_NETWORK
- NOA_MERIDIAN
- NOA_ABBR
- NOA_UNIQUE_3DIG_NATL_NUM
- NOA_ANI
- NOA_NO_ANI_REC'D

- NOA_NON_UNIQUE_SUBSCRIBER
- NOA_NON_UNIQUE_NATIONAL
- NOA_NON_UNIQUE_INTERNATIONAL
- NOA_OPRREQ_TREATED
- NOA_OPRREQ_SUBSCRIBER
- NOA_OPRREQ_NATIONAL
- NOA_OPRREQ_INTERNATIONAL
- NOA_OPRREQ_NO_NUM
- NOA_CARRIER_NO_NUM
- NOA_950_CALL
- NOA_TEST_LINE_CODE
- NOA_INT_INBOUND
- NOA_NAT_OR_INTL_CARRIER_ACC_CODE_INC
- NOA_CELL_GLOBAL_ID_GSM
- NOA_CELL_GLOBAL_ID_NMT_900
- NOA_CELL_GLOBAL_ID_NMT_450
- NOA_CELL_GLOBAL_ID_AUTONET
- NOA_PORTED_NUMBER
- NOA_PISN_SPECIFIC_NUMBER
- NOA_UK_SPECIFIC_ADDRESS
- NOA_SPARE
- NOA_SUBSCRIBER_OPERATOR_REQUESTED
- NOA_NATIONAL_OPERATOR_REQUESTED
- NOA_INTERNATIONAL_OPERATOR_REQUESTED
- NOA_NO_NUMBER_PRESENT_OPERATOR_REQUESTED
- NOA_NO_NUMBER_CUT_THROUGH_TO_CARRIER
- NOA_950_PUBLIC_HOTEL_LINE
- NOA_TEST_CALL
- NOA_MCI_VNET
- NOA_INTERNATIONAL_OPERATOR_TO_OPERATOR_OUTSIDE_WZI
- NOA_INTERNATIONAL_OPERATOR_TO_OPERATOR_INSIDE_WZI
- NOA_DIRECT_TERMINATION_OVERFLOW
- NOA_ISN_EXTENDED_INTERNATIONAL_TERMINATION
- NOA_TRANSFER_ISN_TO_ISN
- NOA_CREDIT_CARD
- RESERVED

Step 5 Specify the Numbering Plan Indicator (NPI) setting for the called party by selecting a value from the called party's Numbering Plan Indicator drop-down list box. The following values are valid for this field.

- NPI_E164 (default value)
- NPI_NONE
- NPI_DATA
- NPI_TELEX
- NPI_PNP
- NPI_NATIONAL
- NPI_TELEPHONY
- NPI_MARITIME_MOBILE
- NPI_LAND_MOBILE
- NPI_ISDN_MOBILE

Step 6 Specify the called number in the called numbers field.

Step 7 Specify the calling number in the calling numbers field.

Step 8 Specify the level of the trace by selecting a value from the trace level drop-down list box. The following values are valid for this list.

- result (default)—Returns the originating trunk group number, called and calling party numbers, outgoing called and calling party numbers, and the resulting trunk group. This trace type is suited for quick call analysis.

Here is an example result trace:

```
>simWriter -tgnum 7001 -isdnp 1 -cdnoa 4 -cdnpi 1 -cdpn 7075511234 -cgpn 7034843
368
>Result of Execution
Originating side: A-number      7034843368
                  B-number      7075511234
                  Trunk group    7001
Outgoing side:   A-number      7034843368
                  B-number      7075511234
                  No suitable trunk group found!
*Internal errors/warnings were encountered during translation!
>OK
```

- diagnostic—Returns limited information about all of the stages of number and route analysis and messages and warnings about data files being read and whether or not default values are being used. This trace type is suited for determining which results were used to produce the outgoing numbers and trunk group.

Here is an example diagnostic trace:

```
>simWriter -tgnum 7001 -isdnp 1 -cdnoa 4 -cdnpi 1 -cdpn 7075511234 -cgpn 7034843
368 -diag
>Result of Execution

*****
* START call translation verification diagnostic summary *
*****

    performing Dial Plan Base.
    performing Profile Analysis (NOA).
*Internal errors/warnings were encountered during translation!

*****
```

```

* END call translation verification diagnostic summary *
*****
Analysing .dat files:
used default Route Preference
used default Terminating Max Digits
used default Terminating Min Digits
used default Originating Min Digits
used default Originating Max Digits
the Originating Start Index property for tg-7001 was not found in /opt/CiscoMGC/
etc/properties.dat
Customer Group ID's do not match up in the sigPath and Properties files
used default Carrier Screening property
used default AOCEnabled field
used the default field for default directory number
used the default Database Access Error flag
Analysis complete, writing message...
Message completed, running simulator...
>OK

```

- full—Returns complete information about all of the stages of number and route analysis. It also includes all tables and parameters from flat files and internal errors generated during generic analysis. This trace type is suited for determining where in the dial plan or number analysis problems occurred.

Here is an example full trace:

```

>simWriter -tgnum 7001 -isdnp 1 -cdnoa 4 -cdnpi 1 -cdpn 7075511234 -cgpn 7034843
368 -full
>Result of Execution

```

```

*****
* START full call translation verification *
*****
Decoding generic analysis trace...
the length of the trace is 82 bytes
( 1)entering Dial Plan Base.
( 2) tracing Dial plan, entering Dial Plan Base table with...
( 1) 0 parameter(s):
( 2) reading Dial Plan Base table...
( 1) 1 error/warning code read:
*Internal Error:Table could not be read
( 1)ending Dial Plan Base...
( 1)entering Call Information Reception.
(13) A Number:'7034843368'
(13) B Number:'7075511234'
( 1)ending Call Information Reception...
( 1)entering Profile Analysis (NOA).
(13) Tracing call number:'7075511234' (Called party number)
( 7) Trace for customer:'jst1'
( 5) TreeBase:'10'
( 2) tracing Dial plan, entering NOA table with...
( 1) 1 parameter(s):
( 4) NOA table index = 4.
( 2) reading NOA table...
( 1) 1 error/warning code read:
*Internal Error:Table could not be read
( 1)ending Profile Analysis (NOA)...
( 1)end of trace reached

*****
* DONE full call translation verification *
* with 0 bytes left untranslated *
*****
Analysing .dat files:

```

```
used default Route Preference
used default Terminating Max Digits
used default Terminating Min Digits
used default Originating Min Digits
used default Originating Max Digits
the Originating Start Index property for tg-7001 was not found in /opt/CiscoMGC/
etc/properties.dat
Customer Group ID's do not match up in the sigPath and Properties files
used default Carrier Screening property
used default AOCEnabled field
used the default field for default directory number
used the default Database Access Error flag
Analysis complete, writing message...
Message completed, running simulator...
>OK
```

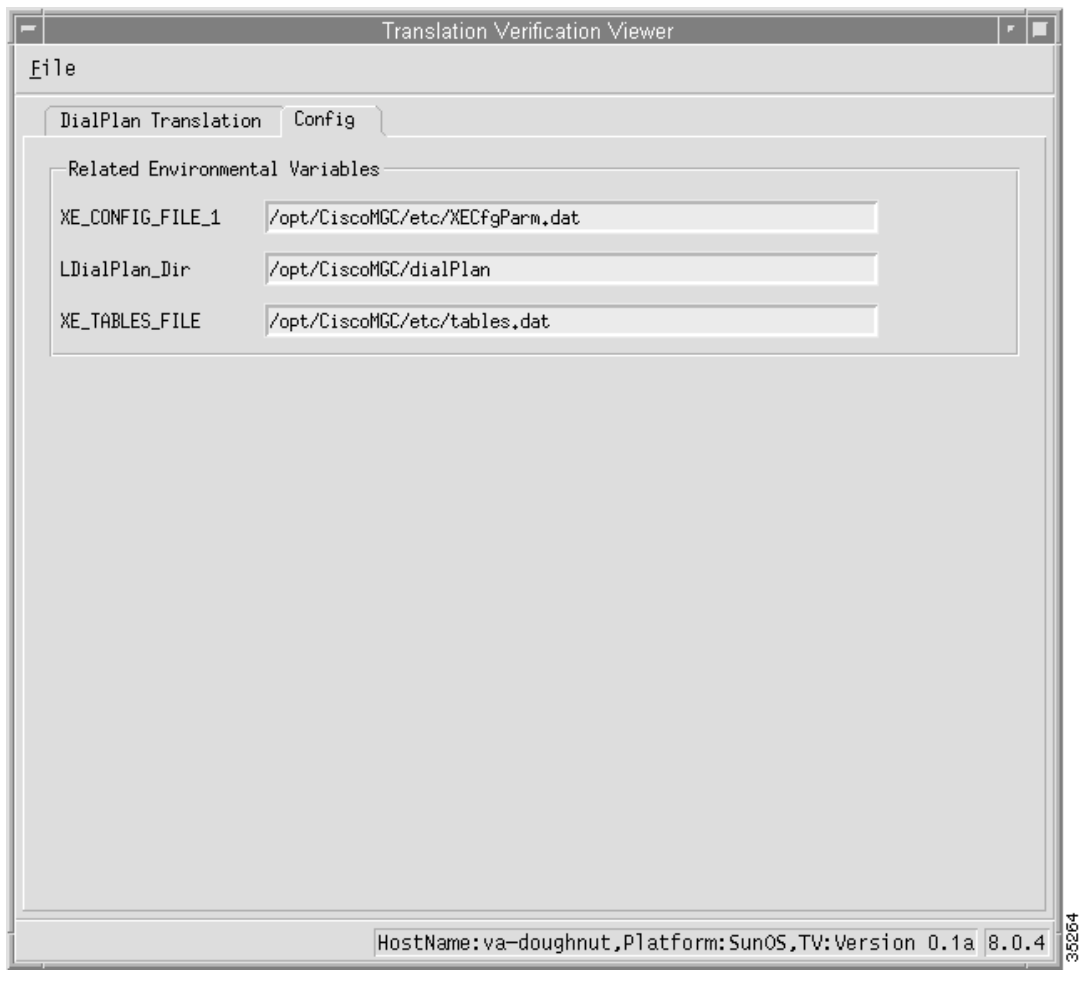
The content of the field identifies for you which elements of your dial plan need to be modified, if necessary.

- Step 9** Click **Execute** to perform a dial plan translation verification. The results are displayed in the field at the bottom of the window.
 - Step 10** If you want to verify additional dial plan translations, repeat steps 2 to 9. The newly requested data is inserted after the old data. Scroll down through the field to view the data you have added. You can clear the display field by clicking **Clear** before you click **Execute**, if you no longer require the previously requested data.
 - Step 11** If you want to save the displayed data, click **SaveinFile**. The contents of the field are saved to a file specified in the XECfgParms.dat file.
-

Viewing Dial Plan Translation Configuration Data

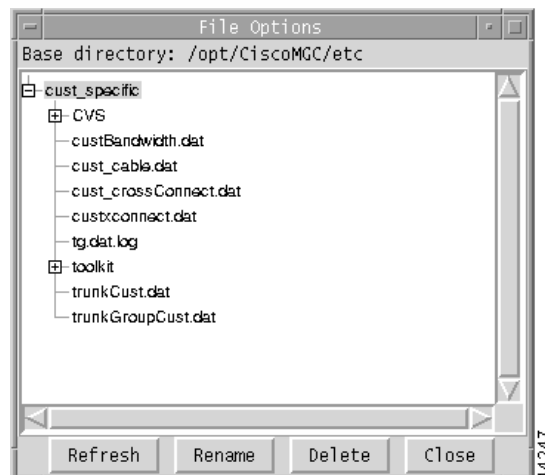
Complete the following steps to view the dial plan translation configuration data:

- Step 1** Open the translation verification viewer. To do this, click **Translation Verification** on the Cisco MGC Toolbar. A popup window displays warning you that running this tool can impact system performance and asking you if you want to launch the tool. Click **Yes**. The Translation Verification Viewer window loads and displays the DialPlan Translation tab window by default (Figure 3-11).
- Step 2** Click the **Config** tab to display the Config tab window (Figure 3-12). The fields in this window display the directory paths to the files used by this viewer. The values in these fields cannot be modified.

Figure 3-12 Config Tab Window

Using the File Options Viewer

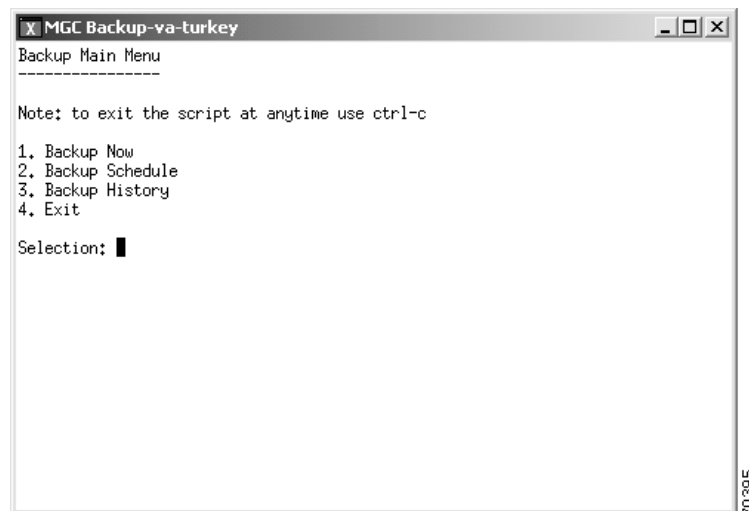
The file options viewer (Figure 3-13) enables you to manage (rename, delete) the files within the \$BASEDIR/etc/cust_specific/toolkit directory. This directory contains all files created by the various toolkit applications. It also enables you to manage subdirectories created under the cust_specific directory. These subdirectories are created through the MML export feature and contain configuration information in the form of MML commands.

Figure 3-13 File Options Viewer Window

Using the MGC Backup Viewer

The MGC backup viewer enables you to backup the software configuration of your Cisco MGC host. For more information on using the MGC backup utility, refer to the “Backup Procedures for Cisco MGC Software from Release 7.4(11) and up” section on page 3-33.

Figure 3-14 illustrates the main window for the MGC backup viewer.

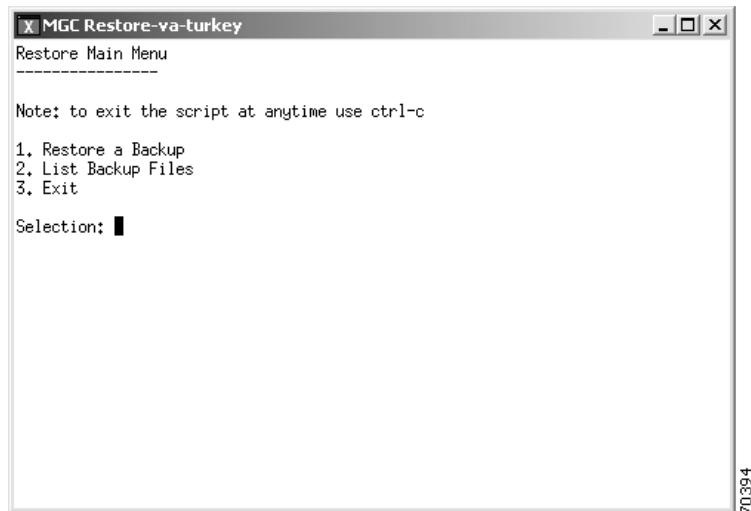
Figure 3-14 MGC Backup Viewer Window

Using the MGC Restore Viewer

The MGC restore viewer enables you to restore a previously stored configuration to your Cisco MGC host. For more information on using the MGC restore utility, refer to the “Restoring Procedures for Cisco MGC Software Release 7.4(11) and up” section on page 8-121.

Figure 3-15 illustrates the main window for the MGC backup viewer.

Figure 3-15 MCG Restore Viewer Window





Maintenance and Troubleshooting Overview

This chapter contains an overview of maintenance and troubleshooting concepts for the elements of the Cisco Media Gateway Controller (MGC) node. It includes overall maintenance and system troubleshooting strategies, and reviews available troubleshooting tools.

Although maintenance and troubleshooting are described separately in this chapter, they are associated activities. Hence, several of the maintenance and troubleshooting chapters in this guide frequently refer to each other.

This chapter includes the following sections:

- Maintenance Strategy Overview, page 4-1
- Troubleshooting Strategy Overview, page 4-2

Maintenance Strategy Overview

Maintenance usually consists of the following tasks for each element of the Cisco MGC node, performed in the order listed:

- Checking equipment status. Determining the current status involves three basic activities:
 - Reading LEDs—Most Cisco products include light-emitting diode (LED) indicators on the front or rear panels and, in some cases, on both panels. These LEDs indicate the status of the equipment. The specific meaning of each LED on each product is described in the maintenance sections for the individual elements of the Cisco MGC node.
 - Issuing Status Queries—You can query the status of the system using various commands. The commands that can be used to determine the status of the devices in your system are described in the maintenance sections for the individual elements of the Cisco MGC node.
 - Using a GUI NMS—Using a network management system (NMS) with a graphical user interface (GUI), such as CiscoWorks2000 or Cisco WAN Manager, to determine the operational status of system devices is described in detail in the maintenance sections for the individual elements of the Cisco MGC node.
- Removing the device from the system—Procedures for removing defective devices from the system with as little impact on the system as possible are described in the maintenance sections for the individual elements of the Cisco MGC node.
- Replacing the complete device—Reinstating a device into the system using a new or repaired model, again with as little impact on the system as possible, is described in the maintenance sections for the individual elements of the Cisco MGC node.

- Replacing hardware components—Swapping out components of a device is a maintenance task used for replacing defective components and for upgrading hardware. The maintenance chapters for each element of the Cisco MGC node include sections describing how to replace the field-replaceable components of that device.

Troubleshooting Strategy Overview

The Cisco MGC node supports connections to external switches and to internal components, such as media gateway controllers, signal processors, and trunking gateways. Because the Cisco MGC node functions in a complex environment involving numerous connections, links, and signaling protocols, when connectivity and performance problems occur, they can be difficult to resolve.

Troubleshooting usually consists of determining the nature of a problem and then isolating the problem to a particular device or component. When a problem has been isolated and identified, troubleshooting also consists of fixing the problem, usually by replacing the device or some component of the device. The goal of this is to provide you with a general troubleshooting strategy, as well as information about the tools available for isolating and resolving connectivity and performance problems.

Symptoms, Problems, and Solutions

Problems in a system are characterized by certain symptoms. These symptoms can be general (such as a Cisco SLT being unable to access the SS7 network) or specific (routes not appearing in a routing table).

You can determine the cause of a symptom by using specific troubleshooting tools and techniques. After identifying the cause, you can correct the problem by implementing a solution consisting of a series of actions.

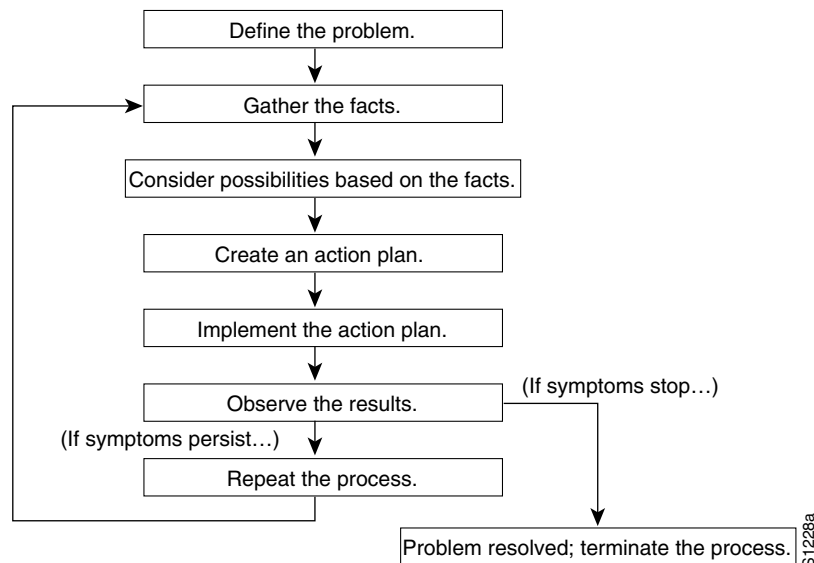
General Problem-Solving Model

A systematic approach works best for troubleshooting. Define the specific symptoms, identify all potential problems that could be causing the symptoms, then systematically eliminate each potential problem (from the most likely to the least likely) until the symptoms are no longer present.

Figure 4-1 illustrates the process flow for this general approach to problem-solving. This process is not a rigid outline for troubleshooting. It is a guide you can use to troubleshoot a problem successfully.

The following steps describe the problem-solving process outlined in Figure 4-1 in more detail:

-
- Step 1** When analyzing a problem, draft a clear problem statement. Define the problem in terms of a set of symptoms and the potential causes behind those symptoms.
- For example, the symptom might be that the EQPT FAIL alarm has become active. Possible causes might be physical problems, a bad interface card, or the failure of some supporting entity (for example, layer 1 framing).
- Step 2** Gather the facts you need to help isolate the symptoms and their possible causes.
- Ask questions of affected users, network administrators, managers, and other key people. Collect information from sources such as network management systems, protocol analyzer traces, output from router diagnostic commands, or software release notes.

Figure 4-1 General Problem-Solving Model

Step 3 Consider possible causes based on the facts you have gathered. You can also use these facts to eliminate potential causes from your list.

For example, depending on the data, you might be able to eliminate hardware as a cause, allowing you to focus on software. At every opportunity, try to narrow the number of potential causes so that you can create an efficient plan of action.

Step 4 Create an action plan based on the remaining potential causes. Begin with the most likely cause, and devise a plan in which only one variable at a time is manipulated.

This approach allows you to reproduce the solution to a specific problem. If you alter more than one variable simultaneously, identifying the change that eliminated the symptom becomes more difficult.

Step 5 Perform each step of the action plan carefully, and test to see if the symptom disappears.

Step 6 Whenever you change a variable, gather the results. You should use the same method of gathering facts that you used in Step 2.

Analyze the results to determine if the problem has been resolved. If it has, then the process is complete.

Step 7 If the problem has not been resolved, you must create an action plan based on the next most likely problem in your list. Return to Step 2 and continue the process until the problem is solved.

Before trying out a new cure, make sure to undo any "fixes" you made in implementing your previous action plan. Remember that you want to change only one variable at a time.



Note

If you exhaust all of the common causes and actions (those outlined in this chapter and those that you have identified for your environment), your last recourse is to contact the Cisco Technical Assistance Center (TAC). Refer to the "Obtaining Technical Assistance" section on page xviii for more information about contacting the Cisco TAC.

System Troubleshooting Tools

This section presents information about the wide variety of tools you can use to troubleshoot the system.

Alarms

The Cisco MGC software generates alarms to indicate problems with processes, routes, linksets, signaling links, and bearer channels. For more information on troubleshooting using alarms, refer to Chapter 8, “Troubleshooting the Cisco MGC Node.” Refer to the *Cisco Media Gateway Controller Software Release 7 Software Messages Reference Guide* for detailed information on the system alarms.

Call Traces

The Cisco MGC generates call traces that capture call-processing activity by following the call from a specified destination through the Cisco MGC software engine to see where it fails. Call failure location is determined using the following information provided in the call trace:

- The protocol data units (PDUs) that the Cisco MGC receives
- How the Cisco MGC decodes the PDU
- The PDUs that the Cisco MGC sends out

The results of call traces are signal flow diagrams that you can use for troubleshooting. Call traces are typically used to capture system activity as part of a procedure to clear an alarm. For more information on using call traces, refer to Chapter 8, “Troubleshooting the Cisco MGC Node.”

System Logs

The Cisco MGC software continuously generates log files of various system information, including operational measurements (OMs) and alarm records. You can use these logs to obtain statistical information about the calls processed by the system and network events such as delays or service-affecting conditions. The Cisco MGC generates the following types of logs:

- Platform logs containing information useful for tracking configuration errors and signaling link and call instantiation problems.
- Command/response logs containing Man-machine language (MML) command history.
- Alarm logs containing alarm information.
- Measurement logs containing system measurements data.
- Call record logs containing call-processing data.

System logs can be read using the various viewers within the Cisco MGC viewer toolkit. For more information on the viewers that comprise the Cisco MGC toolkit, refer to “Using the Cisco MGC Viewer Toolkit” section on page 3-102.

Refer to Appendix A, “Configuring Cisco MGC Report Files,” for more information on system log files.

MML Queries

MML is the command line interface method for configuring and managing the Cisco MGC. You can use it to retrieve information about system components, and to perform logging and tracing. Refer to the *Cisco Media Gateway Controller Software Release 7 Software MML Command Reference Guide* for more information.

Cisco Internetwork Management Tools

The following Cisco internetwork management products provide design, monitoring, and troubleshooting tools to help you manage your Cisco MGC node:

- CiscoWorks2000
- Cisco WAN Manager
- Cisco Media Gateway Controller Node Manager (CMNM)

CiscoWorks2000

CiscoWorks2000 is a series of SNMP-based internetwork management software applications. CiscoWorks applications are integrated on several popular network management platforms. The applications build on industry-standard platforms to provide tools for monitoring device status, maintaining configurations, and troubleshooting problems.

Some of the applications included in CiscoWorks2000 that are useful for troubleshooting are:

- Device Monitor—Monitors specific devices for environmental and interface information.
- Health Monitor—Displays information about the status of a device, including buffers, CPU load, memory available, and protocols and interfaces being used.
- Show Commands—Enables you to view data similar to output from router show EXEC commands.
- Path Tool—Collects path utilization and error data by displaying and analyzing the path between devices.
- Device Polling—Extracts data about the condition of network devices.
- CiscoView—Provides dynamic monitoring and troubleshooting functions, including a graphical display of Cisco devices, statistics, and comprehensive configuration information.
- Offline Network Analysis—Collects historical network data for offline analysis of performance trends and traffic patterns.
- CiscoConnect—Allows you to provide Cisco with debugging information, configurations, and topology information to speed resolution of network problems.

CiscoWorks2000 can be used to manage a variety of Cisco products. Within the Cisco MGC node, CiscoWorks2000 can be used for management of the Cisco SLTs and the Cisco Catalyst 5500 MSRs. Refer to the CiscoWorks2000 documentation for more information.

Cisco WAN Manager

Cisco WAN Manager is part of the Cisco Service Management System of provisioning and management tools for service provider and large enterprise networks. Working at the network and element management level, WAN Manager provides fault-management capabilities handled through the Event Browser, CiscoView, and Configuration Save and Restore features.

You can use Cisco WAN Manager to perform search, sort, and filter operations and to tie events to extensible actions. For instance, Cisco WAN Manager can page someone upon receiving a certain type of SNMP trap. It supports alarm hierarchies that report the root cause of problems to operators and higher-level systems.

Configuration Save and Restore saves a snapshot of the entire network configuration. For disaster recovery, operators can selectively restore configurations of any element, from a single node up to the entire network. This restoration ability significantly reduces recovery time when a catastrophic failure occurs.

The Cisco WAN Manager Trivial File Transfer Protocol (TFTP) statistics collection facility offers the ability to obtain extensive usage and error data across machines and platforms.

A wide range of statistics are available at the port and virtual channel level including:

- Connection statistics
- Circuit line statistics
- Packet line statistics
- Frame Relay port statistics
- Network statistics
- Physical layer statistics
- Protocol layer statistics

The Cisco WAN Manager application can be used to manage a variety of Cisco products. Within the Cisco MGC node, the Cisco WAN Manager can be used for management of the Cisco SLTs and the Cisco Catalyst 5500 MSRs. Refer to the Cisco WAN Manager documentation for more information.

Cisco Media Gateway Controller Node Manager

The Cisco Media Gateway Controller Node Manager (CMNM) is an element management system based on the Cisco Element Management Framework (CEMF). It is responsible for managing the Cisco MGC node, including Cisco MGC(s), LAN switch(es), and Cisco SLTs.

NMS design divides network management into five discrete areas: fault, configuration, accounting, performance, and security. The CMNM provides fault and performance management of the Cisco MGC, as well as flow-through provisioning of the Cisco MGC and its subcomponents. In addition, CMNM also provides fault and performance management of the Cisco SLT and LAN switch. CMNM uses the Cisco Voice Service Provisioning Tool to provide configuration of the Cisco MGC and uses CiscoView for configuration of the Cisco SLT and the LAN switch.

Security and some accounting features are provided directly by the CEMF platform. CMNM does not provide any security or accounting features beyond what is natively supported by the CEMF. CMNM is designed to be used on a standalone basis with a customer operations support system or a Cisco-based NMS such as the Voice Network Manager (VNM).

For more information on CMNM, refer to the *Cisco MGC Node Manager User's Guide*.

Cisco SLT Diagnostic Commands

Cisco SLTs provide the following integrated IOS command types to assist you in monitoring and troubleshooting systems:

- **show**
- **debug**
- **ping**
- **trace**

Show Commands

The show commands are powerful monitoring and troubleshooting tools. You can use the show commands to perform a variety of functions:

- Monitoring router behavior during initial installation
- Monitoring normal network operation
- Isolating problem interfaces, nodes, media, or applications
- Determining when a network is congested
- Determining the status of servers, clients, or other neighbors

Some of the most commonly used status commands include:

- **show interfaces**—Displays statistics for network interfaces using the following commands:
 - **show interfaces ethernet**
 - **show interfaces fddi**
 - **show interfaces atm**
 - **show interfaces serial**
- **show controller t1**—Displays statistics for T1 interface card controllers
- **show running-config**—Displays the router configuration currently running
- **show startup-config**—Displays the router configuration stored in nonvolatile RAM (NVRAM)
- **show flash**—Displays the layout and contents of Flash memory
- **show buffers**—Displays statistics for the buffer pools on the router
- **show memory**—Shows statistics about the router's memory, including free pool statistics
- **show processes**—Displays information about the active processes on the router
- **show stacks**—Displays information about the stack utilization of processes and interrupt routines, as well as the reason for the last system reboot
- **show version**—Displays the configuration of the system hardware, the software version, the names and sources of configuration files, and the boot images

For details on using and interpreting the output of specific **show** commands, refer to the Cisco IOS command reference for the release you are using.

Using Debug Commands

The **debug** privileged EXEC commands can provide a wealth of information about the traffic being seen (or not seen) on an interface, error messages generated by nodes on the network, protocol-specific diagnostic packets, and other useful troubleshooting data.



Caution

Exercise care when using **debug** commands. These commands are processor-intensive and can cause serious network problems (degraded performance or loss of connectivity) if they are enabled on an already heavily loaded router. When you finish using a **debug** command, remember to disable it with its specific **no debug** command, or use the **no debug all** command to turn off all debugging.

**Note**

Output formats vary among **debug** commands. Some generate a single line of output per packet, and others generate multiple lines of output per packet. Some generate large amounts of output, and others generate only occasional output. Some generate lines of text, and others generate information in field format.

To minimize the negative impact of using **debug** commands, follow this procedure:

- Step 1** Enter the **no logging console** global configuration command on your router. This command disables all logging to the console terminal.
- Step 2** Telnet to a router port and enter the **enable EXEC** command.
- Step 3** Enter the **terminal monitor** command on your router to copy **debug** command output and system error messages to your current terminal display.

This permits you to view **debug** command output remotely, without being connected through the console port. Following this procedure minimizes the load created by using **debug** commands because the console port no longer has to generate character-by-character processor interrupts.

If you intend to keep the output of the **debug** command, spool the output to a file. The procedure for setting up such a **debug** output file, as well as complete details regarding the function and output of **debug** commands is provided in Chapter 10, “Debug Command Reference,” in the *Troubleshooting Internetworking Systems* manual.

**Note**

In many situations, third-party diagnostic tools can be more useful and less intrusive than the use of **debug** commands. For more information, see the “Third-Party Troubleshooting Tools” section on page 4-9.

Using the Ping Command

To check host accessibility and network connectivity, use the **ping** EXEC (user) or privileged EXEC command.

For IP, the **ping** command sends ICMP Echo messages. If a station receives an ICMP Echo message, it sends an ICMP Echo Reply message back to the source. The extended command mode of the **ping** command permits you to specify the supported IP header options. This allows the router to perform a more extensive range of test options.

It is a good idea to use the **ping** command when the network is functioning properly under normal conditions so that you have something to compare against when you are troubleshooting.

For detailed information on using the **ping** and extended **ping** commands, refer to the *Cisco IOS Configuration Fundamentals Command Reference*.

Using the Trace Command

The **trace** user EXEC command discovers the routes a router's packets follow when traveling to their destinations. The **trace** privileged EXEC command permits the supported IP header options to be specified, allowing the router to perform a more extensive range of test options. The **trace** command uses the error message generated by routers when a datagram exceeds its time-to-live (TTL) value.

First, probe datagrams are sent with a TTL value of 1. This causes the first router to discard the probe datagrams and send back "time exceeded" error messages. The **trace** command then sends several probes and displays the round-trip time for each. After every third probe, the TTL is increased by 1.

Each outgoing packet can result in one of two error messages. A "time exceeded" error message indicates that an intermediate router has seen and discarded the probe. A "port unreachable" error message indicates that the destination node has received the probe and discarded it, because it could not deliver the packet to an application. If the timer goes off before a response comes in, the **trace** command prints an asterisk (*).

The **trace** command terminates when the destination responds, when the maximum TTL is exceeded, or when the user interrupts the **trace** with the escape sequence. It is a good idea to use the **trace** command when the network is functioning properly under normal conditions so that you have something to compare against when troubleshooting.

For detailed information on using the **trace** and extended **trace** commands, refer to the *Cisco IOS Configuration Fundamentals Command Reference*.

Third-Party Troubleshooting Tools

In many situations, third-party diagnostic tools can be more useful than system commands that are integrated into the router. For example, the enabling of a processor-intensive **debug** command can contribute to the overloading of an environment that is already experiencing excessively high traffic levels. Attaching a network analyzer to the suspect network is less intrusive and is more likely to yield useful information without interrupting the operation of the router.

Some useful third-party tools for troubleshooting internetworks include:

- Volt-ohm meters, digital multimeters, and cable testers
- Breakout boxes, fox boxes, bit error rate testers (BERTs), and block error rate testers (BLERTs)
- Network analyzers and network monitors
- Time domain reflectometers (TDRs) and optical time domain reflectometers (OTDRs)

Volt-Ohm Meters, Digital Multimeters, and Cable Testers

Volt-ohm meters and digital multimeters are at the lower end of the spectrum of cable testing tools. These devices can measure basic parameters such as AC and DC voltage, current, resistance, capacitance, and cable continuity. They are used primarily to check physical connectivity.

Cable testers (scanners) can also be used to check physical connectivity. Cable testers are available for shielded twisted-pair, unshielded twisted-pair, 10BASE-T, and coaxial and twinax cables.

A given cable tester might be also able to perform any of the following functions:

- Test and report on cable conditions, including near-end crosstalk, attenuation, and noise
- Perform TDR, traffic monitoring, and wire map functions
- Display media access control (MAC) layer information about LAN traffic, provide statistics such as network utilization and packet error rates, and perform limited protocol testing (for example, TCP/IP tests such as ping)

Similar testing equipment is available for fiber-optic cable. Due to the relatively high cost of fiber-optic cable and its installation, the cable should be tested both before installation (on-the-reel testing) and after installation. Continuity testing of fiber-optic cable requires either a visible light source or a

reflectometer. Light sources capable of providing light at the three predominant wavelengths, 850 nanometers (nm), 1300 nm, and 1550 nm, are used with power meters that can measure the same wavelengths and test attenuation and return loss in the fiber-optic cable.

Breakout Boxes, Fox Boxes, and BERTs/BLERTs

Breakout boxes, fox boxes, and BERTs/BLERTs are digital interface testing tools used to measure the digital signals present at the interfaces of PCs, CSU/DSUs, and other devices. These testing tools can monitor data line conditions, analyze and trap data, and diagnose problems common to communications systems. Traffic from data terminal equipment (DTE) through data communications equipment (DCE) can be examined so that you can isolate problems, identify bit patterns, and ensure that the proper cabling has been installed. These devices cannot test media signals such as those for Ethernet, Token Ring, or FDDI.

Network Monitors and Analyzers

You can use network monitors to continuously track packets crossing a network, thus obtaining an accurate picture of network activity at any moment, or a historical record of network activity over a period of time. Network monitors do not decode the contents of frames. Monitors are useful for baselining, in which the activity on a network is sampled over a period of time to establish a normal performance profile or baseline.

Monitors collect information such as packet sizes, numbers of packets, error packets, overall usage of a connection, the number of hosts and their MAC addresses, and details about communications between hosts and other devices. You can use the data to create profiles of LAN traffic as well locate traffic overloads, plan for network expansion, detect intruders, establish baseline performance, and distribute traffic more efficiently.

A network analyzer (also called a protocol analyzer) decodes the various protocol layers in a recorded frame and presents them as readable abbreviations or summaries, detailing which layer is involved (physical, data link, and so forth) and what function each byte or byte content serves.

Most network analyzers can perform many of the following functions:

- Filtering traffic that meets certain criteria so that, for example, all traffic to and from a particular device can be captured
- Time-stamping captured data
- Presenting protocol layers in an easily readable form
- Generating frames and transmitting them onto the network
- Incorporating an "expert" system in which the analyzer uses a set of rules, combined with information about the network configuration and operation, to diagnose and solve, or offer potential solutions to, network problems

TDRs and OTDRs

TDRs are at the top end of the cable testing spectrum. These devices can quickly locate open and short circuits, crimps, kinks, sharp bends, impedance mismatches, and other defects in metallic cables.

A TDR works by "bouncing" a signal off the end of the cable. Opens, shorts, and other problems reflect the signal back at different amplitudes, depending on the problem. A TDR measures how much time it takes for the signal to reflect and calculates the distance to a fault in the cable. TDRs can also be used to measure the length of a cable or calculate the propagation rate based on a configured cable length.

Fiber-optic measurement is performed by an OTDR. OTDRs can accurately measure the length of the fiber, locate cable breaks, measure the fiber attenuation, and measure splice or connector losses. An OTDR can be used to ascertain the "signature" of a particular installation, noting attenuation and splice losses. This baseline measurement can then be compared with future signatures when a problem in the system is suspected.



Maintaining the Cisco MGC

This chapter contains the recommended hardware maintenance procedures for the Cisco Media Gateway Controller (MGC). The Cisco MGC performs call-processing, trunk resource management, alarm management, and routing. Cisco MGCs also provide various Cisco telephony solutions with Advanced Intelligent Network (AIN) capabilities, including the ability to detect conditions that cause the Cisco MGC to query service logic for further call-processing instructions. Cisco MGCs can be installed in simplex or continuous service configurations. In simplex configurations, only one Cisco MGC is equipped. In continuous service configurations, two Cisco MGCs are equipped. Only one Cisco MGC is active at any given time in a continuous service configuration, while the other Cisco MGC operates in standby mode. The Cisco MGC runs on a variety of Sun Netra UNIX systems.

This chapter briefly describes hardware maintenance for the Cisco MGC. For more detailed information, refer to the documentation provided by Sun Microsystems for your hardware platform. For information on upgrading and maintaining Cisco MGC software, refer to the *Cisco Media Gateway Controller Software Release 7 Installation and Configuration Guide*.

This chapter includes the following sections:

- Checking Equipment Status, page 5-1
- Maintaining Technical Support Staff, page 5-3
- Maintaining Components, page 5-3

Checking Equipment Status

You can quickly check the status of the Cisco MGC by using the following methods:

- Reading the LEDs
- Querying the system using UNIX and Man-Machine Language (MML) commands

The UNIX and MML commands for querying the status of the system are found in “Cisco MGC Node Operations” section on page 3-1. Information about the LEDs on the Cisco MGC hosts is found in the sections that follow.

Sun Netra LEDs

The Sun Netra t 1120/1400 and Sun Netra t 1125/1405 display the following LEDs:

- POWER—Green LED is illuminated at all times when the system is on.

- **SYSTEM**—Green LED is off (or reset) during power-up procedures and is illuminated when UNIX is running and the alarms driver is installed. This LED is reset by a hardware Watchdog timeout, or when the user-defined Alarm3 (spare) is asserted.
- **ALARM1**—Amber LED is illuminated when the user-defined Alarm 1 is asserted.
- **ALARM2**—Amber LED is illuminated when the user-defined Alarm 2 is asserted.
- **SPARE**—Amber LED is reserved for future enhancement.

The DC-powered Sun Netra t 1120/1400 displays the following additional LEDs:







- **SUPPLY A**—Green LED is illuminated when DC input A is present and the system is powered on.
- **SUPPLY B**—Green LED is illuminated when DC input B is present and the system is powered on.

Sun Enterprise 450 LEDs

The Sun Enterprise 450 platform is no longer being offered. However, customers upgrading their MGC software to Release 7 might be using this platform. For this reason, information on the LEDs for this platform is provided.

Table 5-1 describes the LEDs, and their associated icons, for the Sun Enterprise 450 platform.

Table 5-1 LED Descriptions for the Sun Enterprise 450 Platform

| Name | Icon | Description |
|--------------------|---|---|
| Power-on |  | This green LED lights steadily while the system power is on and the keyswitch is in the On, Diagnostics, or Locked position. |
| General fault |  | This yellow LED blinks slowly while the system runs its power-on self-test (POST) diagnostics and blinks rapidly during OpenBoot diagnostics (OB DIAG) tests. It lights steadily when any fault is detected (including a fault also reported by another LED). |
| Activity |  | This green LED blinks continuously if the system is operating normally. |
| Disk fault |  | This yellow LED lights steadily if there is a fault in one of the hard disk drives. When this LED is lit, one or more disk LEDs might also be lit, indicating the source of the fault. |
| Temperature fault |  | This yellow LED lights steadily if there is an over-temperature condition in the system or a faulty fan assembly. |
| Power supply fault |  | This yellow LED lights steadily if there is a fault in one of the power supplies. When this LED is lit, LEDs on the rear of each power supply indicate the source of the fault. |

Maintaining Technical Support Staff

Skill Level of Personnel

The engineering staff must collectively have training specific to the Sun Netra to support the product in the field. To be classified as “certified” by Sun, support personnel must successfully complete the Sun certification training courses and pass the Solaris administrator’s certification examinations.

All engineers must be able to perform the following tasks:

- User assistance
- Problem diagnosis and duplication
- Hardware replacement
- Patch distribution

The technical profile portion of the Sun audit analyzes the technical ability of service personnel and determines if the number of support staff is sufficient for quality customer support.

Staff Software Troubleshooting Tools

The support engineers must have a current version of Sunsolve to assist in troubleshooting and resolving problems.

Maintaining Components

For more detailed information, see the *Cisco Media Gateway Controller Hardware Installation Guide*.

Software Upgrades

Refer to the *Cisco Media Gateway Controller Software Release 7 Installation and Configuration Guide* for a description of the procedures for software upgrades.



Maintaining the Cisco Signaling Link Terminal

This chapter contains the recommended hardware maintenance procedures for the Cisco Signaling Link Terminal (SLT), which is designed to perform SS7 signal pre-processing for a Cisco Media Gateway Controller. The Cisco SLT consists of a custom Cisco IOS image running on a Cisco 2611 router. For information on upgrading and maintaining Cisco SLT software, refer to the *Cisco Signaling Link Terminal* documentation.

As part of an end-to-end telephony solution, the Cisco SLT provides reliable transport of Signaling System 7 (SS7) protocols across an IP network. The Cisco SLT uses the Cisco IOS SS7 Cisco SLT feature set, providing reliable interoperability with the Cisco Media Gateway Controller (MGC). The Cisco SLT uses Cisco's Reliable User Datagram Protocol (RUDP) to backhaul upper-layer SS7 protocols across an IP network.

When used for Signal Link Terminal applications, the modular Cisco 2611 dual Ethernet port router can be configured with dual serial as well as Multiflex WAN interface cards with integrated E1 data service units (DSUs) or T1 channel service units (CSUs)/DSUs. For additional flexibility, the Multiflex WAN interface cards can also be ordered with a dual-port Drop and Insert capability.

The following interface cards are supported:

- 1-port high-speed serial interface (WIC-1T)
- 2-port high-speed serial interface (WIC-2T)
- 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)

Only SS7 serial interfaces and protocols are supported. There is no support for non-SS7 serial WAN protocols. Only two SS7 signaling links are supported per Cisco SLT, and only one SS7 signaling link is supported per T1 or E1 port.



Note

Presently, only one Ethernet port of the Cisco 2611 is supported for Cisco SLT communications with the Cisco MGC.

This chapter describes Cisco SLT hardware maintenance and includes the following sections:

- Checking Equipment Status, page 6-2
- Removing a Cisco SLT, page 6-5
- Replacing a Cisco SLT, page 6-6
- Replacing Hardware Components, page 6-13
- Additional Maintenance Tasks, page 6-15

Checking Equipment Status

You can check the status of the Cisco SLT devices using the following methods:

- Reading Cisco SLT LEDs
- Using Cisco IOS status queries
- Using CiscoWorks 2000, Cisco WAN Manager, or the Cisco MGC Node Manager (CMNM)

Cisco SLT LEDs

LEDs indicate the current operating condition of the Cisco SLT.

Front-Panel LEDs

Figure 6-1 shows the location of the LEDs on the Cisco SLT. Table 6-1 describes these LEDs.

Figure 6-1 Cisco SLT Front-Panel LEDs

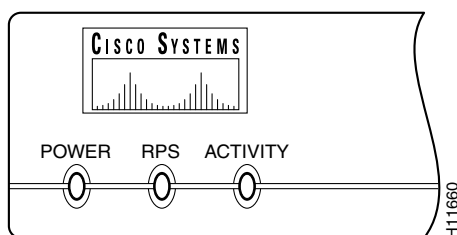


Table 6-1 Cisco SLT Front-Panel LEDs

| LED | Description |
|-------|--|
| Power | Indicates the Cisco SLT operating status. Goes on when power is supplied to the Cisco SLT and the Cisco SLT is operational. |
| RPS | <p>OFF—No RPS¹ is attached.</p> <p>ON—RPS is attached and operational.</p> <p>Blink—RPS is attached, but has a failure.</p> |

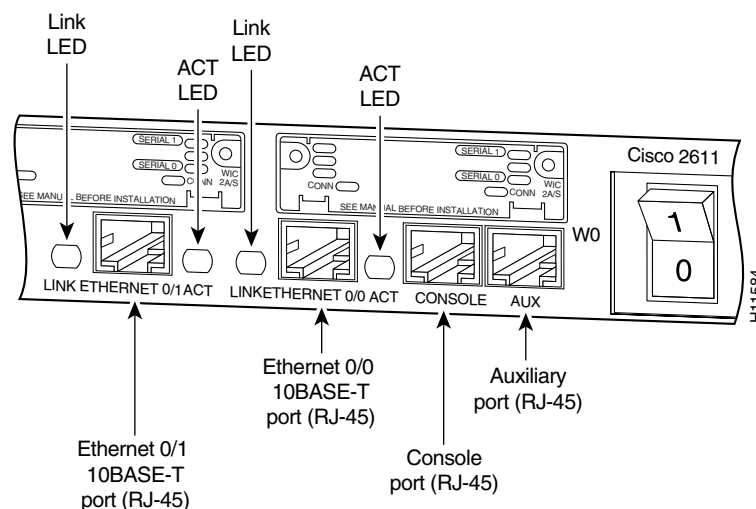
Table 6-1 Cisco SLT Front-Panel LEDs (continued)

| LED | Description |
|----------|--|
| Activity | <p>OFF—In the Cisco IOS software, but no network activity.</p> <p>Blink (500 ms ON, 500 ms OFF)—In Remote Monitor (ROMMON), no errors.</p> <p>Blink (500 ms ON, 500 ms OFF, 2 sec. between codes)—In ROMMON, error detected.</p> <p>Blink (less than 500 ms)—In the Cisco IOS software, the blink rate reflects the level of activity.</p> |

1. RPS = Redundant Power System.

Rear-Panel LEDs

Figure 6-2 shows the location of the Cisco SLT rear-panel LEDs. Table 6-2 describes these LEDs.

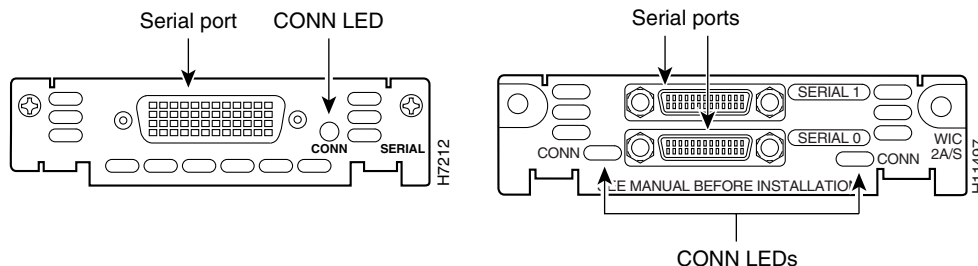
Figure 6-2 Cisco SLT Rear-Panel LEDs**Table 6-2 Cisco SLT Rear-Panel LEDs**

| LED | Description |
|------|---|
| Link | When this LED is lit, a link has been established with the hub or switch at the other end of the cable. |
| ACT | When this LED is lit, packets are being transmitted or received on the Ethernet interface. |

WIC LEDs

Each serial card has one LED, labeled CONN for each port, which lights when the serial port is connected. When the port is in DTE mode, the CONN LED indicates that Data Set Ready (DSR), Data Carrier Detect (DCD), and Clear To Send (CTS) have been detected. When the port is in DCE mode, it indicates that Data Terminal Ready (DTR) and Request To Send (RTS) have been detected.

Figure 6-3 1- and 2-Port Serial WAN Interface Card LEDs



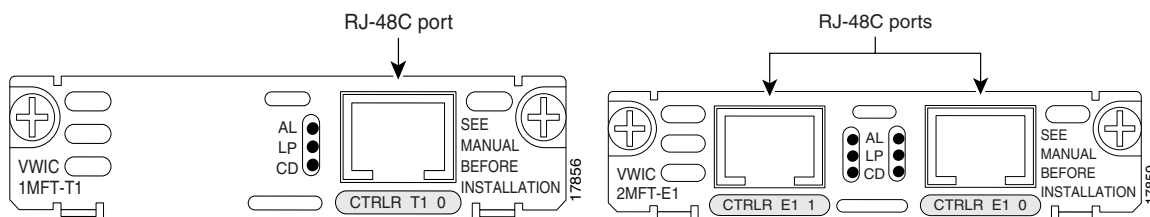
VVIC LEDs

You can distinguish between T1 and E1 interface cards by the labeling on the faceplate, as shown in Figure 6-4. Each multiflex trunk interface card has three LEDs, which are shown in Figure 6-4 and described in Table 6-3.

Table 6-3 1-Port Multiflex Trunk Interface Card LEDs

| LED | Description | Color |
|--------|---|--------|
| LP LED | On means that a loopback or line state is detected or is manually set by the user. This LED is off during normal operation. | Yellow |
| AL LED | On means that there is a local or remote alarm state. This LED is off during normal operation. | Yellow |
| CD LED | On means that a carrier has been detected and the internal DSU/CSU in the WAN interface card is communicating with another DSU/CSU. This LED is on during normal operation. | Green |

Figure 6-4 1- and 2-Port T1 and E1 Multiflex Trunk Interface Card LEDs



Using the Cisco SLT Operating System to Check Status

The Cisco SLT operating system includes a series of commands that enable you to determine if the unit is functioning correctly or where problems have occurred. A few of the relevant commands for checking status are listed here. To learn how to find more information concerning these and other IOS commands, refer to the *Cisco IOS Software Documentation Organization*.

Status commands that may help to monitor the health and state of your Cisco SLT at any given time include the following:

- **show c2600**—Shows complex troubleshooting information that does not pertain to a specific interface, but to the platform's shared resources.
- **show context**—Displays information stored in nonvolatile random access memory (NVRAM) when an exception occurs.
- **show flash**—Shows information about the Flash memory device.
- **show interfaces**—Displays statistics for all interfaces configured on the Cisco SLT.
- **show ip route**—Displays the entries in the routing table.
- **show mem**—Shows statistics about the unit's memory, including memory free pool statistics.
- **show processes**—Displays information about the active processes.
- **show protocols**—Displays the configured protocols. This command shows the status of any configured Layer 3 (network) protocol.
- **show rudp failures**—Displays Reliable User Datagram Protocol (RUDP) failure statistics.
- **show rudp statistics**—Displays RUDP internal statistics.
- **show running-config**—Displays the active configuration parameters.
- **show SS7 mtp2**—Displays Message Transfer Part 2 (MTP 2) channel control-block data, MTP 2 link state information, MTP 2 statistics, MTP 2 timer information, protocol information for a channel, and the channel number. (The default is channel 0.)
- **show SS7 sm**—Displays session manager session information.
- **show startup-config**—Displays the backup configuration file.
- **show version**—Displays the configuration of the system hardware, the software version, the names and sources of configuration files, and the boot images.

**Note**

The SS7-related commands (**show SS7 mtp2**, **show SS7 sm**, **show rudp failures**, and **show rudp statistics**) are part of Cisco's RUDP session manager. They are not available on other Cisco equipment running IOS.

Removing a Cisco SLT

This section describes how to shut down a Cisco SLT and remove it. The assumption is that the system has been properly installed according to procedures described in the *Cisco Media Gateway Controller Hardware Installation Guide*, most notably the following procedures:

- Safety recommendations
- General site requirements
- Preparations for connecting to the network

Required Tools and Equipment

Following are the tools and parts that might be required for removing a Cisco SLT:

- Number 2 Phillips screwdriver
- Flat-blade screwdrivers: small, 3/16-inch (0.476 cm) and medium, 1/4-inch (0.625 cm)

- ESD-preventive wrist strap

It is also assumed that the cables and console terminal were installed during the original system installation.

Procedure

To remove the Cisco SLT, complete the following steps:

-
- | | |
|---------------|--|
| Step 1 | Power off the Cisco SLT. |
| Step 2 | Attach the ESD-preventive wrist strap to the chassis of the Cisco SLT. |
| Step 3 | Disconnect all cables from the rear panel of the Cisco SLT. |
| Step 4 | Remove the front and rear mounting screws and remove the unit from the rack. |
-

Replacing a Cisco SLT

This section describes how to install a new Cisco SLT or reinstall a repaired Cisco SLT.

Required Tools and Equipment

Following are the tools and parts that might be required for replacing a Cisco SLT:

- Number 2 Phillips screwdriver
- Flat-blade screwdrivers: small, 3/16-inch (0.476 cm) and medium, 1/4-inch (0.625 cm)
- ESD-preventive wrist strap
- Screws to secure the rack-mount brackets to the Cisco SLT

It is assumed that cables, Ethernet hub, and the console terminal remain from the original installation.

Mounting the Chassis in a Rack

This section describes the procedures for rack-mounting the chassis. A new chassis comes with brackets for use with a 19-inch rack or, if specified in your order, optional larger brackets for use with a 24-inch rack. The brackets are shown in Figure 6-5.



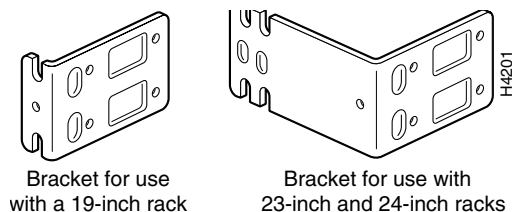
Warning

To prevent bodily injury when mounting or servicing this unit in a rack, you must take special precautions to ensure that the system remains stable. The following guidelines are provided to ensure your safety:

- If the rack contains only one unit, mount the unit at the bottom of the rack.
- If the rack is a partially filled rack, load the rack from the bottom to the top, with the heaviest component at the bottom of the rack.

- If the rack contains stabilizing devices, install the stabilizers prior to mounting or servicing the unit in the rack.

Figure 6-5 Identifying the Brackets



Attaching the Brackets

To install the chassis in a rack, attach the brackets in one of the following ways:

- With the front panel forward (see Figure 6-6 and Figure 6-7)
- With the rear panel forward (see Figure 6-8 and Figure 6-9)
- In a center-mount rack, with the rear panel forward (see Figure 6-10)



Note

Use the Cisco-supplied screws for this installation.



Note

If you are installing a Cisco SLT in a 19-inch rack with a 17.5-inch opening, orient the rack-mount brackets so that, when installed, they do not increase the width of the chassis. (See Figure 6-6.)

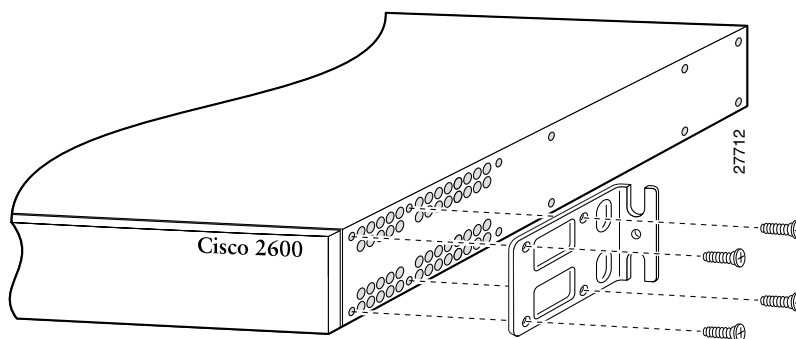
If you are installing a Cisco SLT in a 19-inch EIA-standard rack with a 17.75-inch opening or a 23- or 24-inch rack, orient the rack-mount brackets so that, when installed, they increase the width of the chassis. (See Figure 6-7.)



Note

The following illustrations show how to connect the bracket to one side of the chassis. The second bracket connects to the opposite side of the chassis.

Figure 6-6 Bracket Installation—Front Panel Forward (19-Inch Rack with a 17.5-Inch Opening)



Note: The second bracket attaches to the other side of the chassis.



Note

When installed in a 19-inch rack with a 17.75-inch opening, the Cisco SLT protrudes beyond the front of the rack.

Figure 6-7 Bracket Installation—Front Panel Forward (19-Inch Rack with a 17.75-Inch Opening or a 23-inch or 24-Inch Rack)

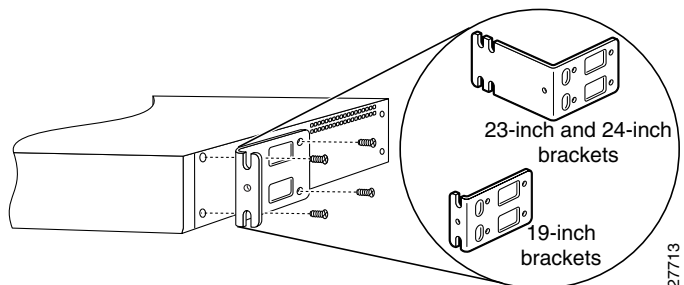


Figure 6-8 Bracket Installation—Rear Panel Forward (19-Inch Rack with a 17.5-Inch Opening)

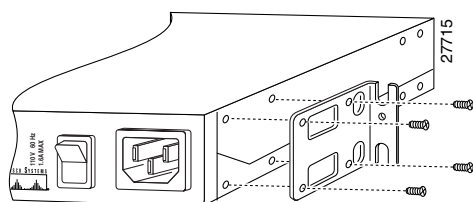


Figure 6-9 Bracket Installation—Rear Panel Forward (19-Inch Rack with a 17.75-Inch Opening or a 23-inch or 24-Inch Rack)

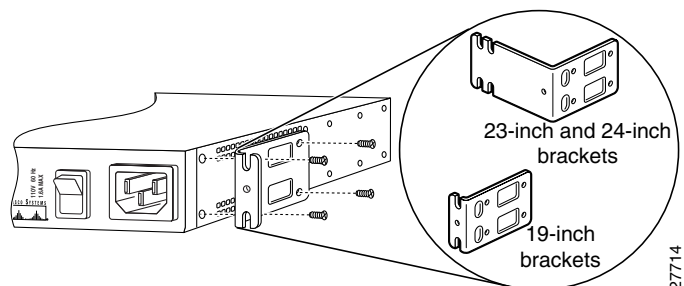
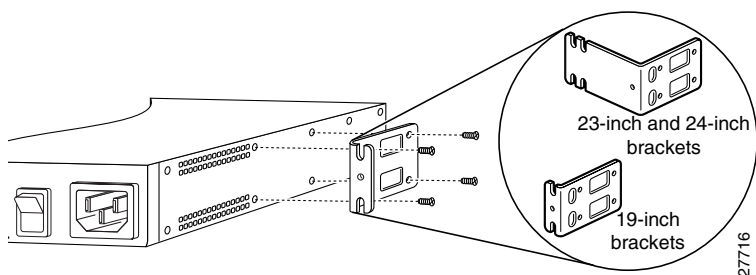


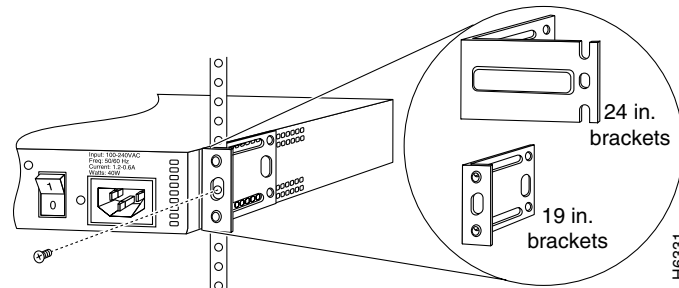
Figure 6-10 Center-Mount Bracket Installation—Rear Panel Forward



Installing the Cisco SLT in a Rack

After the brackets are secured to the chassis, you can rack-mount the Cisco SLT. Using the screws you provide, attach the chassis to the rack as shown in Figure 6-11.

Figure 6-11 Attaching the Chassis to a Rack—Rear Panel Forward



Connecting the DC Power Supply

This section describes the DC power supply specifications and wiring.



This unit is intended for installation in restricted access areas. A restricted access area is where access can only be gained by service personnel through the use of a special tool, lock and key, or other means of security, and is controlled by the authority responsible for the location.

DC Power Specifications

The DC power supply is intended for use in DC-operating environments. Table 6-4 lists the power supply specifications.

Table 6-4 Power Supply Specifications

| Description | Design Specification |
|----------------------------------|----------------------|
| Power (input) | 40W, -38 to -75 VDC |
| Wire gauge for power connections | 14 AWG ¹ |

1. AWG = American Wire Gauge.

Wiring the DC Power Supply

If you ordered a Cisco SLT with a DC power supply, follow the directions in this section to wire the terminal block.



Before performing any of the following procedures, ensure that power is removed from the DC circuit. To ensure that all power is OFF, locate the circuit breaker on the panel board that services the DC circuit, switch the circuit breaker to the OFF position, and tape the switch handle of the circuit breaker in the OFF position.

**Warning**

Figure 6-12 shows the DC power supply terminal block. The proper wiring sequence is ground to ground, positive to positive (line to L), and negative to negative (neutral to N). Note that the ground wire should always be connected first and disconnected last.

**Caution**

Do not over torque the terminal block captive thumbscrew or terminal block contact screws. The recommended torque is 8.2 ± 0.4 inch-lb.

**Warning**

After wiring the DC power supply, remove the tape from the circuit breaker switch handle and reinstate power by moving the handle of the circuit breaker to the ON position.

**Warning**

Secure all power cabling when installing this unit to avoid disturbing field-wiring connections.

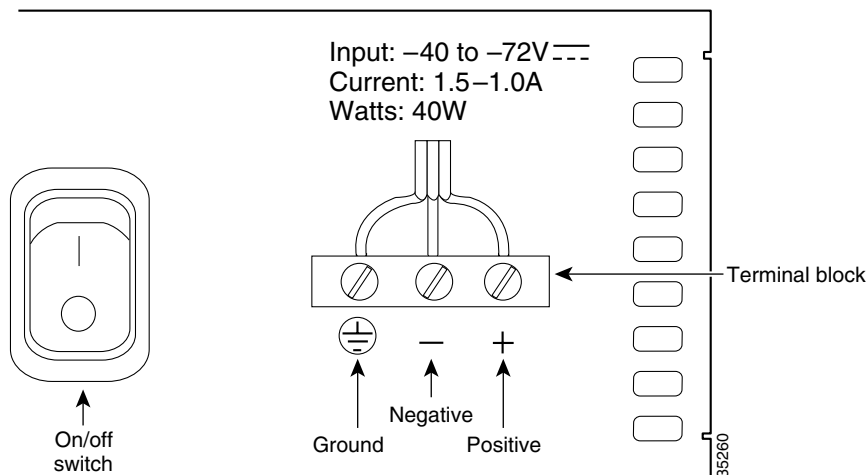
**Note**

This product is intended for installation in restricted access areas and is approved for use with 14 AWG copper conductors only. The installation must comply with all applicable codes.

To wire the terminal block, complete the following steps:

- Step 1** Attach the appropriate lugs at the wire end of the power supply cord.
- Step 2** Wire the DC power supply to the terminal block, as shown in Figure 6-12.

Figure 6-12 DC Power Supply Connections



Connecting to a Network

This section explains how to connect the Cisco SLT to the control signaling LAN. It is assumed that the cables required to connect the Cisco SLT to the LAN are available from the Cisco SLT being replaced.

**Warning**

Do not work on the system, or connect or disconnect cables during periods of lightning activity.

Connect the Ethernet 10BaseT port to an Ethernet 10BaseT port on the LAN switch.

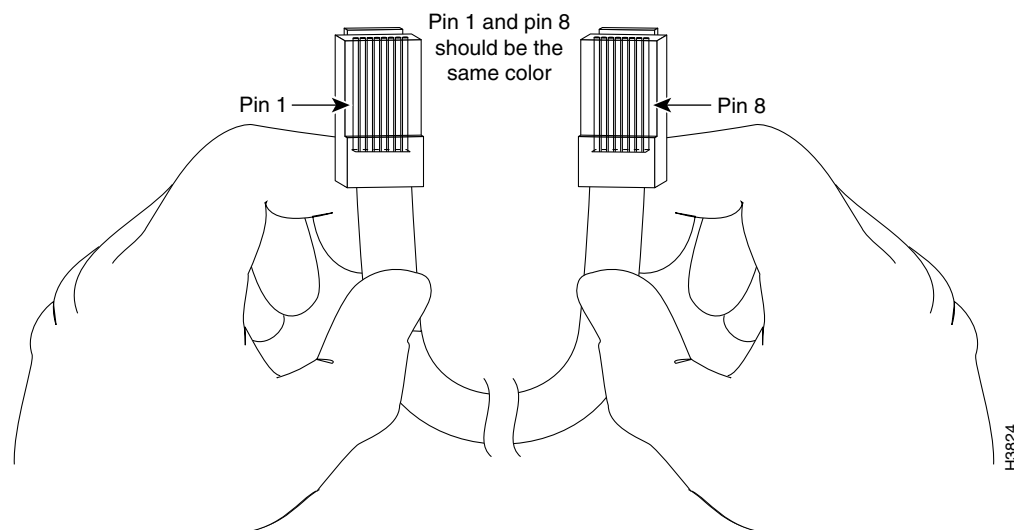
Connecting the Console Terminal and Modem

Cisco SLTs include asynchronous serial console and auxiliary ports. These ports provide local administrative access to your Cisco SLT (with a console terminal) or remote access (with a modem).

Identifying a Rollover Cable

Use a rollover cable to connect to the asynchronous serial console and auxiliary ports. You can identify a rollover cable by comparing the two modular ends of the cable. When you hold the two cable ends side-by-side with the tab at the back, as shown in Figure 6-13, the wire connected to the pin on the outside of the left plug should be the same color as the wire connected to the pin on the outside of the right plug. If your cable came from Cisco Systems, pin 1 is white on one connector, and pin 8 is white on the other (a rollover cable reverses pins 1 and 8, 2 and 7, 3 and 6, and 4 and 5).

Figure 6-13 *Identifying a Rollover Cable*



H3824

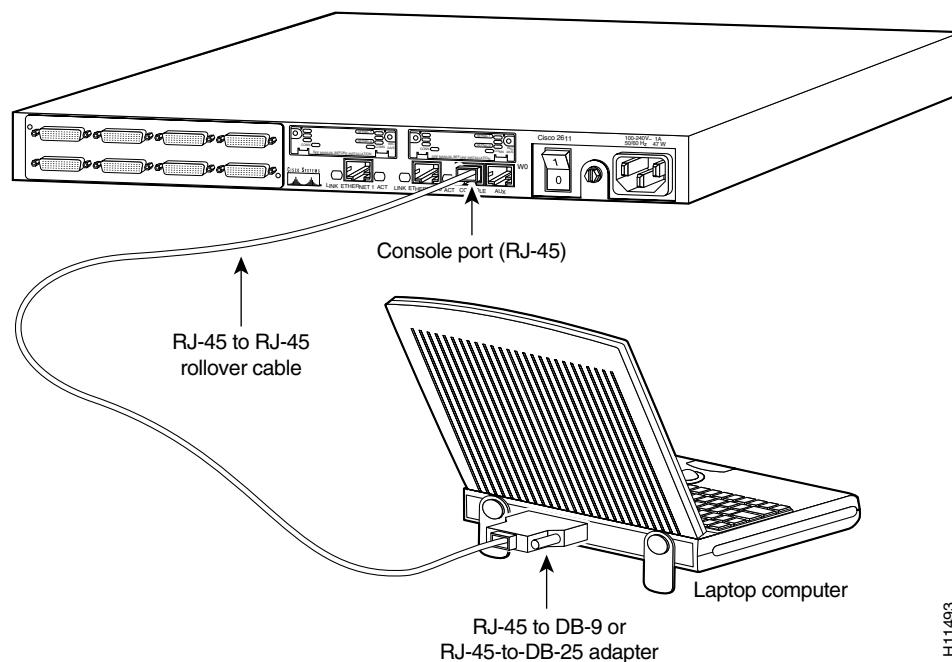
Connecting to the Console Port

Take the following steps to connect a terminal (an ASCII terminal or a PC running terminal emulation software) to the console port on the Cisco SLT:

- Step 1** Connect the terminal using the thin, flat, RJ-45-to-RJ-45 rollover cable (looks like a telephone cable) and an RJ-45-to-DB-9 or RJ-45-to-DB-25 adapter (labeled TERMINAL) included with the Cisco SLT. (See Figure 6-14.)
- Step 2** Configure your terminal or PC terminal emulation software for 9600 baud, 8 data bits, no parity, and 2 stop bits.

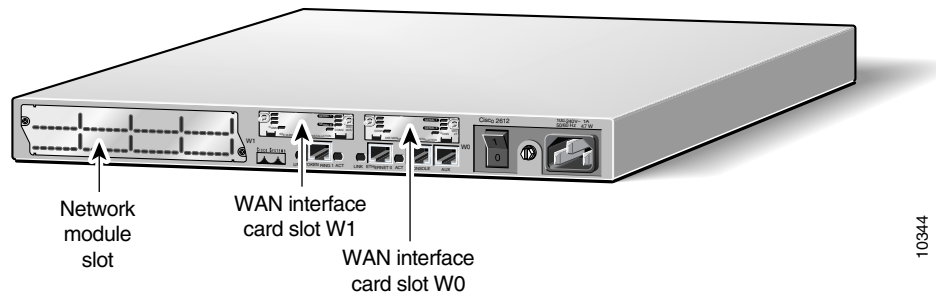
For information on console port pinouts, see the online document *Cisco Modular Access Router Cabling Specifications* on the Documentation CD-ROM that accompanied your Cisco SLT package.

Figure 6-14 Connecting a Console Terminal



Cisco SLT Interface Numbering

Each individual network interface on a Cisco SLT is identified by a slot number and a unit number. The Cisco SLT chassis contains one slot in which you can install a network module. Figure 6-15 shows the slot location in the Cisco SLT chassis.

Figure 6-15 Cisco SLT WAN Interface Card Chassis Slot Locations

Unit numbers identify the interfaces on the modules installed in the unit. Unit numbers begin at 0 for each interface type, and continue from right to left and from bottom to top. Modules are identified by interface type, slot number (always 0), a forward slash (/), then the unit number. For example:

- First Ethernet interface is referred to as Ethernet 0/0
- Slot W0, serial interface 0 is referred to as serial 0/0
- Slot W1, serial interface 1 is referred to as serial 0/1

**Note**

WAN interface card slots (built into the chassis) are always numbered as slot 0, even if the interface card is installed in the slot labeled W1. For information about WAN interface slot and port numbering, see the *Cisco WAN Interface Cards Hardware Installation Guide*.

Install the New Software

After you have installed the Cisco SLT, power it on. (If the Cisco SLT does not power on, proceed to Appendix B, “Troubleshooting Cisco SLT Signaling.”)

After the hardware has been installed and powered on, you must configure the Cisco SLT. Refer to the *Cisco Media Gateway Controller Software Release 7 Installation and Configuration Guide*.

After the Cisco SLT has been configured, you must install a special release of the Cisco IOS software on the Cisco SLT. The filename of the current Cisco SLT image is c2600-ipss7-mz.121-1.T.bin.

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

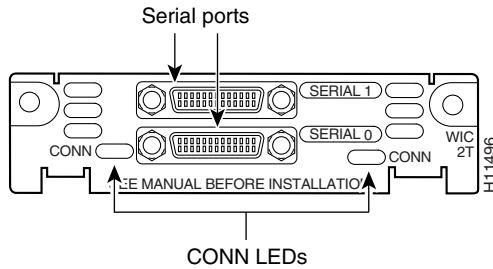
```
copy tftp:[[/location]/directory]/filename flash-filesystem:[filename]
```

Replacing Hardware Components

Each Cisco SLT is equipped with at least one WAN interface card. This section describes how to replace the WAN interface cards in the Cisco SLTs, and contains the following subsections:

- Required Tools and Equipment, page 6-14
- Installing a WAN Interface Card, page 6-14

Figure 6-16 shows the WIC-2T WAN interface card.

Figure 6-16 WIC-2T Dual Port Serial WAN Interface Card

Required Tools and Equipment

In addition to the WIC and the Cisco SLT, you will need these items to install and connect your card:

- Number 1 Phillips screwdriver.
- Appropriate connecting cable—The cables should already be available. For more information on cable types, see the online document *Cisco Modular Router Cable Specifications* on the Documentation CD-ROM that came with your Cisco SLT package, or on Cisco Connection Online.
- Synchronous modem, channel service unit/data service unit (CSU/DSU), or other data circuit-terminating equipment (DCE) (serial card only)—Used to connect the WAN interface card to a digital WAN line.

Installing a WAN Interface Card

This section describes the procedure for installing a WIC-2T WAN interface card in a Cisco SLT slot.

You can install the WIC-2T either before or after mounting the Cisco SLT, whichever is more convenient. Similarly, you can install the WIC-2T in the network module either before or after installing the network module in the Cisco SLT chassis.



Caution

WICs do not support online insertion and removal (hot-swapping). Before inserting a card into the network module or Cisco SLT chassis, you must turn off electrical power and disconnect network cables.



Warning

Before performing any of the following procedures, ensure that power is removed from the DC circuit. To ensure that all power is OFF, locate the circuit breaker on the panel board that services the DC circuit, switch the circuit breaker to the OFF position, and tape the switch handle of the circuit breaker in the OFF position.

To install WAN interface cards in a Cisco SLT WIC chassis slot, complete the following procedure:

Step 1

Turn off power to the Cisco SLT. However, to channel ESD voltages to ground, do not unplug the power cable. Remove all network interface cables, including telephone cables, from the rear panel.

**Note**

If you are installing a single WIC-2T, use slot W0 first (see Figure 6-15). The Cisco SLT checks slot W0 before it checks slot W1. If you fill slot W1 while leaving slot W0 vacant, your Cisco SLT configuration could be affected.

- Step 2** Use a screwdriver to remove the blank filler panel from the chassis card slot where you plan to install the card. Save the filler panel for future use.
- Align the card with the guides in the WAN interface card slot and slide it gently into the slot.
 - Push the card into place until you feel its edge connector mate securely with the connector in the WAN interface card slot.
 - Fasten the card's captive mounting screws into the holes in the WAN interface card slot, using the screwdriver.
 - Reinstall the network interface cables and turn on power to the Cisco SLT.

The following warning applies only to Cisco SLTs that use a DC power supply:

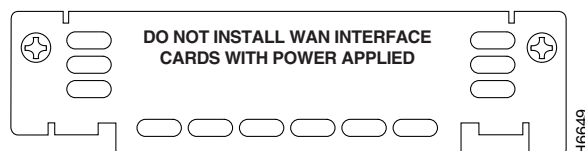
**Warning**

After wiring the DC power supply, remove the tape from the circuit breaker switch handle and reinstate power by moving the handle of the circuit breaker to the ON position.

WIC Filler Panels

If any interface card slot (on the network module or chassis) is unoccupied, install a filler panel to enable proper airflow. (See Figure 6-17.)

Figure 6-17 WIC Slot Filler Panel



Additional Maintenance Tasks

This section contains selected maintenance procedures you might need to perform on a Cisco SLT as your internetworking needs change, including the following:

- Upgrading DRAM, page 6-16
- Opening the Chassis, page 6-16
- Replacing the System-Code SIMM, page 6-19
- Closing the Chassis, page 6-21
- Procedures for Recovering Boot and System Images, page 6-22

Additional maintenance procedures are available on the Documentation CD-ROM that shipped with the Cisco SLT.

To see translated versions of warnings in this section, see the *Regulatory Compliance and Safety Information* document that accompanied your Cisco SLT.

**Caution**

Before opening the chassis, be sure that you have discharged all static electricity from your body and the power is off.

**Warning**

Before working on a chassis or working near power supplies, unplug the power cord on AC units; disconnect the power at the circuit breaker on DC units.

Upgrading DRAM

This section describes how to upgrade dynamic random-access memory (DRAM) on the system card. You might need to upgrade DRAM if you have loaded a new Cisco IOS software feature set or release.

To see how much memory is currently installed in the Cisco SLT, enter the **show version** command. Near the middle of the resulting output, a message similar to the following appears:

```
Cisco 2611(MPC860) processor (revision 0x200) with 28672K/4096K bytes of memory.
```

This line shows how much memory is installed (in this example, 28672 K/4096 K). The first number represents primary memory, and the second number represents shared memory.

For information about recommended DRAM part numbers for your Cisco SLT, refer to the *Cisco 2600 Series Hardware Installation Guide*.

Cisco SLT DRAM

Cisco SLTs contain two 100-pin dual in-line memory module (DIMM) sockets (or banks) for DRAM, numbered 0 and 1. (See Figure 6-20.) Each socket can be filled with a 100-pin DRAM DIMM. You can use the **memory-size iomem** software command to configure DRAM as a mixture of shared memory, which is used for data transmitted or received by network modules and WAN interface cards, and primary or main memory, which is reserved for the CPU. For further information about this command, see the Cisco IOS configuration guides and command references.

Opening the Chassis

This section describes the procedure for opening the chassis by removing the chassis cover.

**Warning**

Do not touch the power supply when the power cord is connected. For systems with a power switch, line voltages are present within the power supply even when the power switch is OFF and the power cord is connected. For systems without a power switch, line voltages are present within the power supply when the power cord is connected.

Tools Required

You will need the following tools to remove and replace the DRAM DIMMs on the Cisco SLT:

- Number 2 Phillips screwdriver
- ESD-preventive wrist strap
- DRAM DIMM required for your planned upgrade

Removing the Chassis Cover

You must open the chassis to access the internal components.



Warning

Before opening the chassis, disconnect the telephone-network cables to avoid contact with telephone-network voltages.

To remove the chassis cover, complete the following steps:

- Step 1** Power off the Cisco SLT.
- Step 2** Disconnect all cables from the rear panel of the Cisco SLT.
- Step 3** Remove the screws located on the top of the chassis. Note that the chassis is composed of two sections, top and bottom.
- Step 4** Holding the chassis with both hands, position it as shown in Figure 6-18.
- Step 5** Slide the top section away from the bottom section as shown in Figure 6-19.

Figure 6-18 Holding Chassis for Cover Removal

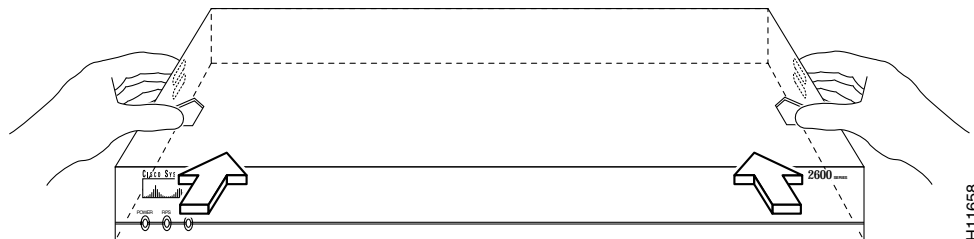
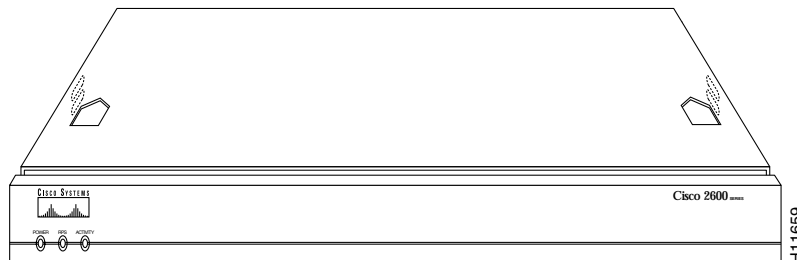
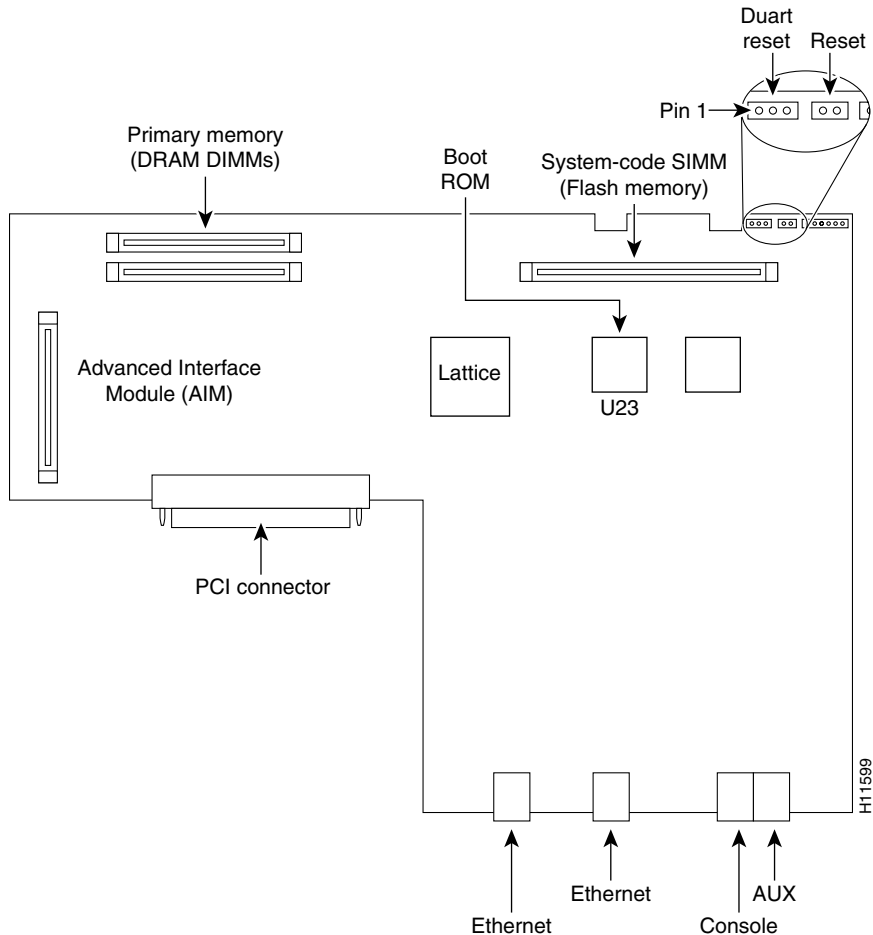


Figure 6-19 Removing Chassis Cover



- Step 6** When the top cover is off, set it aside. Figure 6-20 shows the layout of the system cards.

Figure 6-20 System Card Layout



DRAM DIMM Installation

Take the following steps to install the DRAM DIMMs:

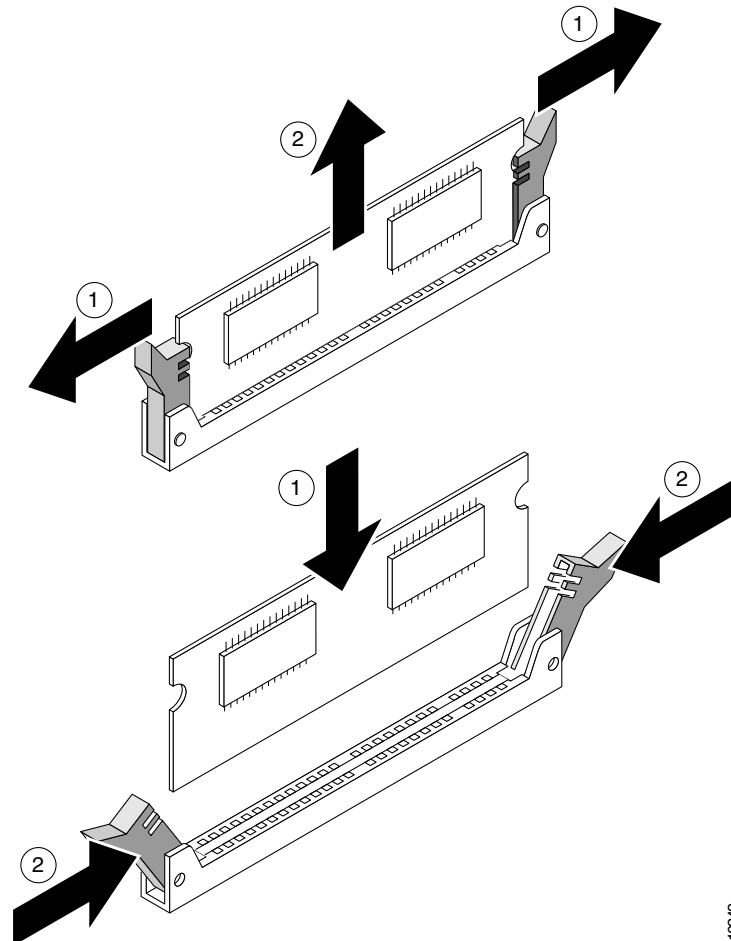
- Step 1** Power off the Cisco SLT.
- Step 2** Attach an ESD-preventive wrist strap.
- Step 3** Open the cover following the instructions in the “Opening the Chassis” section on page 6-16.
- Step 4** Remove the existing DRAM DIMM by pulling outward on the connectors to unlatch them, as shown in Figure 6-21. Be careful not to break the holders on the DIMM connector.



Caution

To prevent damage, do not press on the center of the DIMMs. Handle each DIMM carefully.

- Step 5** Position the new DIMM so that the polarization notch is located at the left end of the DIMM socket as shown in Figure 6-21.

Figure 6-21 Removing and Replacing the DRAM DIMM

10243

- Step 6** Insert the new DRAM DIMM by sliding the end with the metal fingers into the DIMM connector socket at approximately a 90° angle to the system card. Gently rock the DIMM back into place until the latch on either side snaps into place. Do not use excessive force, because the connector might break.
- Step 7** Replace the Cisco SLT cover. Follow the instructions in the “Closing the Chassis” section on page 6-21.

Replacing the System-Code SIMM

The system code (Cisco SLT operating system software) is stored in a Flash memory 80-pin single in-line memory module (SIMM).

For information about recommended SIMM part numbers for your Cisco SLT, refer to the *Cisco 2600 Series Hardware Installation Guide*.

Tools Required

You will need the following tools to remove and replace the system-code SIMM on the Cisco SLT:

- Medium-size flat-blade screwdriver (1/4 inch [0.625 cm])
- Electrostatic discharge (ESD)-preventive wrist strap
- System-code SIMM

Preparing to Install the System-Code SIMM

There is one system-code (Flash memory) SIMM socket on the system board. You can verify how much Flash memory is already installed in your Cisco SLT by entering the **show flash EXEC** command.



Caution

The system code is stored on the Flash memory SIMM, but new system-code SIMMs are shipped without preinstalled software. Before continuing with this procedure, use the **copy flash tftp EXEC** command to back up the system code to a Trivial File Transfer Protocol (TFTP) server.



Note

For more information about the **copy flash tftp** command and other related commands, refer to the Cisco IOS configuration and command reference publications. These publications are available on the Documentation CD-ROM that came with your Cisco SLT, and on Cisco.com.

System-Code SIMM Replacement

Take the following steps to upgrade the system-code Flash memory SIMM:

- Step 1** If you have not already done so, enter the **copy flash tftp EXEC** command to back up the system code.
- Step 2** Power off the Cisco SLT.
- Step 3** Remove all cables from the rear panel of the Cisco SLT.
- Step 4** Attach an ESD-preventive wrist or ankle strap.
- Step 5** Open the chassis cover, following the procedure in the “Opening the Chassis” section on page 6-16.
- Step 6** Locate the system-code SIMM on the system card. (See Figure 6-20.)
- Step 7** If necessary, remove the existing system-code SIMM by pulling outward on the connector holders to unlatch them. The connector holds the SIMM tightly, so be careful not to break the holders on the SIMM connector. (See Figure 6-22.)
- Step 8** Position the new SIMM so that the polarization notch is located at the left end of the SIMM socket.



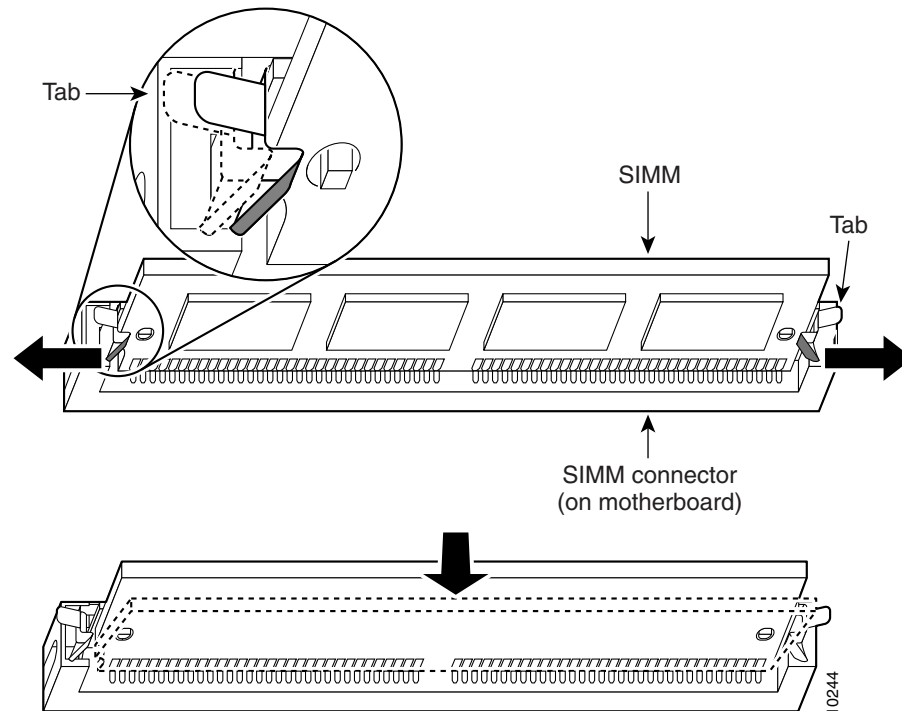
Caution

To prevent damage, do not press on the center of the SIMM. Handle each SIMM carefully. Note that some Flash memory SIMMs have the components mounted on the rear side; therefore, when inserting the SIMM, always use the polarization notch as a reference and *not* the position of the components on the SIMM.

- Step 9** Insert the new SIMM by sliding the end with the metal fingers into the SIMM connector socket at approximately a 90° angle to the system card. Gently rock the SIMM back into place until the latches on both sides snap into place. Do not use excessive force because the connector might break.

- Step 10** Replace the Cisco SLT cover following the procedure in the following section.
- Refer to the “Procedures for Recovering Boot and System Images” section on page 6-22 for instructions on how to place the Cisco IOS image on the new SIMM.

Figure 6-22 Removing and Replacing the System-Code SIMM



Closing the Chassis

This section describes the procedure for closing the chassis by replacing the chassis cover.

Replacing the Cover

To replace the cover, complete the following steps:

- Step 1** Position the two chassis sections, as shown in Figure 6-19.
- Step 2** Referring to Figure 6-18, press the two chassis sections together and ensure that the top section fits *into* the rear of the bottom section, the bottom section fits *into* the front of the top section, and that the sides of the top and bottom sections fit together.
- Caution** To fit the two sections together, it might be necessary to work them together at one end and then the other; however, use care to prevent bending the chassis edges.
- Step 3** When the two sections fit together snugly, slide the chassis top until it fits into the front bezel.

- Step 4** Replace the cover screws. Tighten the screws to no more than 8 or 9 inch/pound of torque.
 - Step 5** Reinstall the chassis on the wall, rack, desktop, or table.
 - Step 6** Reconnect all cables.
-

Procedures for Recovering Boot and System Images

If your Cisco SLT experiences difficulties and no longer contains a valid Cisco IOS software image in Flash memory, you can recover the Cisco IOS image using the procedures described in the *Cisco Signaling Link Controller* documentation.



Maintaining the Cisco Catalyst 5500 Multiswitch Router

This chapter contains recommended hardware maintenance procedures for the Cisco Catalyst 5500 Multiswitch Routers (MSRs), which provide an Ethernet backbone for connections between the Cisco Signaling Link Terminals (SLTs), Cisco Media Gateway Controllers (MGCs), and Cisco Media Gateways (MGWs). You can configure several virtual LANs (VLANs) on the Catalyst 5500s and the route switch modules (RSMs) provide inter-VLAN routing when necessary. If your solution includes two Catalyst 5500s, they are connected through an Inter-Switch Link (ISL) trunk, enabling them to share VLAN data and provide ensured availability.

This chapter describes hardware maintenance; for information on upgrading and maintaining Catalyst 5500 software, refer to the *Cisco Media Gateway Controller Software Release 7 Installation and Configuration Guide*.

This chapter includes the following sections:

- Checking Equipment Status, page 7-1
- Replacing Hardware Components, page 7-5

Checking Equipment Status

Check the status of the Cisco Catalyst 5500, using the following methods:

- Reading the Cisco Catalyst 5500 LEDs
- Querying the status using the Catalyst command line interface (CLI)
- Querying the system using CiscoWorks 2000 and Cisco WAN Manager (CWM)

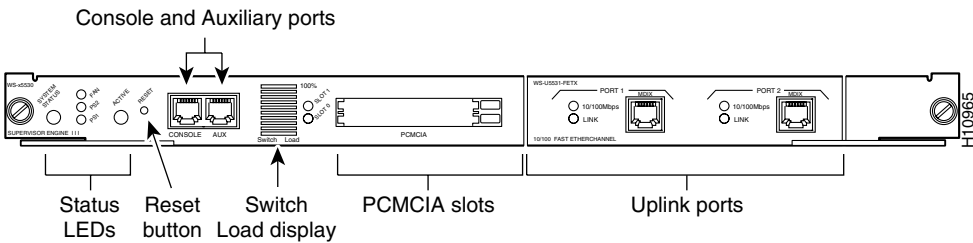
Cisco Catalyst 5500 LEDs

LEDs of the Catalyst 5500 may vary, depending on which components are installed. The LEDs described in this section are factory default.

Supervisor Engine Module LEDs

The front panel of the supervisor engine III (product number WS X5530-E3) is shown in Figure 7-1.

Figure 7-1 Supervisor Engine III Front Panel



The LEDs on the supervisor engine front panel indicate the status of the system, which includes the supervisor engine, the power supplies, and the fan assembly. Table 7-1 describes LED operation.

Table 7-1 Supervisor Engine III and Uplink Module LED Descriptions

| LED | State | Description |
|---------------|--------|---|
| SYSTEM STATUS | Green | Indicates that a series of self-tests and diagnostic tests has been passed. |
| | Red | System is being booted or is faulty (fails a test or module is disabled). |
| | Orange | Fan modules have failed or redundant power supply is installed, but not turned on. |
| FAN | Green | The fan is operational. |
| | Red | The fan is not operational. |
| PS1 | Green | Power supply in left bay is operational. |
| | Red | Power supply in left bay is not operational, switched off, or not receiving power. |
| | Off | Power supply in the left bay is off or not installed.
Note The Catalyst 5500 power supply LED is red when no modules are installed. |
| PS2 | Green | The power supply in the right bay is operational. |
| | Red | The power supply in the right bay is not operational, is switched off, or is not receiving input power. |
| | Off | The power supply in the right bay is off or is not installed.
Note The Catalyst 5500 power supply LED is red when no modules are installed. |
| SWITCH LOAD | 1–100% | If the switch is operational, the switch load display indicates (as an approximate percentage) the current traffic load over the backplane. |
| ACTIVE | Green | The supervisor engine is operational and active. |
| | Orange | The supervisor engine module is in standby mode. |

Table 7-1 Supervisor Engine III and Uplink Module LED Descriptions (continued)

| LED | State | Description |
|-------------------|-----------------|--|
| SLOT 1 and SLOT 0 | On | Supervisor Engine III only: The Flash PC Card SLOT 1 and SLOT 0 LEDs light when their respective slot 1 and slot 0 Flash PC Card devices are accessed. |
| 100 Mbps | Green | The port is operating at 100 Mbps. |
| 1000 Mbps | Green | The port is operating at 1000 Mbps. |
| LINK | Green | The port is operational. |
| | Orange | The link has been disabled by software. |
| | Flashing orange | The link is bad and has been disabled due to a hardware failure. |
| | Off | No signal is detected. |

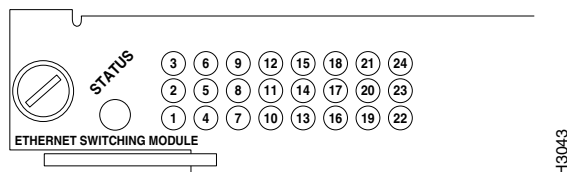
Ethernet Switching Module (10BaseT 24 Port) LEDs

Each switching module (Prod # WS-X5013) contains a STATUS LED. When on, this LED indicates that the switching module is operational and is powered up. It does not necessarily mean that the interface ports are functional or enabled.

The LEDs on the faceplate of the Ethernet switching module (10BaseT 24 Port) are described in Table 7-2 and shown in Figure 7-2.

Table 7-2 Ethernet Switching Module (10BaseT 24 Port) LED Descriptions

| LED | Description |
|--------|--|
| STATUS | <p>The switch performs a series of self-tests and diagnostic tests. If it passes all the tests, the status LED is green.</p> <p>If it fails any test, the status LED is red (or orange for a minor fault or if manually disabled).</p> |
| Link | <p>If the port is operational (a signal is detected), the LED is green.</p> <p>If the link has been disabled by software, the LED is orange.</p> <p>If the link is bad and has been disabled due to a hardware failure, the LED flashes orange.</p> <p>If no signal is detected, the LED is off.</p> |

Figure 7-2 Ethernet Switching Module (10BaseT 24 Port) LEDs

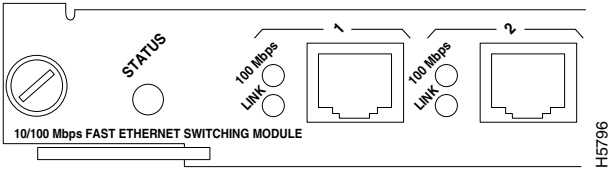
10/100 Mbps Fast Ethernet Switching Module (10/100BaseTX 12 Port) LEDs

The faceplate of each 10/100 Mbps Fast Ethernet Switching Module (Prod # WS-X5203) contains a module STATUS LED, and two LEDs for each switching port. The LEDs provide status information for the module and individual Fast Ethernet interface connections. The LEDs are described in Table 7-3 and are shown in Figure 7-3.

Table 7-3 10/100 Mbps Fast Ethernet Switching Module (10/100BaseTX 12 Port) LEDs

| LED | Description |
|-------------------|--|
| STATUS | <p>The switch performs a series of self-tests and diagnostic tests.</p> <p>If it passes all the tests, the LED is green.</p> <p>If it fails a test other than an individual port test fails, the LED is red.</p> <p>During system boot or if the module is disabled, the LED is orange.</p> <p>During self-test diagnostics, the LED is orange.</p> <p>If the module is disabled, the LED is orange.</p> |
| 100 Mbps | <p>If the port is operating at 100 Mbps, the LED is green.</p> <p>If the port is operating at 10 Mbps, the LED is off.</p> |
| LINK (bottom LED) | <p>If the port is operational (a signal is detected), the LED is green.</p> <p>If the link has been disabled by software, the LED is orange.</p> <p>If the link is bad and has been disabled due to a hardware failure, the LED flashes orange.</p> <p>If no signal is detected, the LED is off.</p> |

Figure 7-3 10/100 Mbps Fast Ethernet Switching Module (10/100BaseTX 12 Port) LEDs



Route Switch Module LEDs

The RSM (product number WS-X5302) LEDs, shown in Figure 7-4, are described in Table 7-3.

Figure 7-4 RSM (WS-X5302) LEDs



Table 7-4 RSM (WS-X5302) STATUS LED Descriptions

| LED | State | Description |
|----------------------|--------|--|
| STATUS | Green | All the self-tests have been passed. |
| | Red | A test other than an individual port test has been failed. |
| | Orange | System boot, self-test diagnostics running, or the module is disabled. |
| CPU HALT | On | Indicates normal RSM operation. |
| | Off | The system detected a processor hardware failure. |
| ENABLED | On | Indicates IP microcode is loaded and the RSM is operational. |
| PCMCIA SLOTS 0 and 1 | On | Indicates PCMCIA devices in slot 0 and 1 are being accessed by the RSM. |
| TX ¹ | Green | The port is transmitting a packet (LED is lit for approximately 50 ms). |
| RX ² | Green | The port is receiving a packet (LED is lit for approximately 50 ms ³). |

1. TX = transmit

2. RX = receive

3. ms = milliseconds

Using the Command Line Interface to Check Status

The Cisco Catalyst 5500 command line interface includes a series of commands that enable you to determine if the MSR is functioning correctly or where problems have occurred. Relevant commands for checking status include **ping**, **traceroute**, **test snmp trap**, and **show**. There are more than 100 **show** commands, many of which can be used to check status. To learn how to find more information concerning these and other commands, refer to the *Command Reference Manual* that came with the Cisco Catalyst 5500 MSR.

Replacing Hardware Components

This section describes how to perform the following removal and replacement procedures for Cisco Catalyst 5000 series field-replaceable units (FRUs):

- Removing the Supervisor Engine, page 7-6
- Using Flash Memory (PCMCIA) Cards (Supervisor Engine III), page 7-7
- Removing and Replacing the Power Supply, page 7-8
- Removing and Replacing the Chassis Fan Assembly, page 7-15

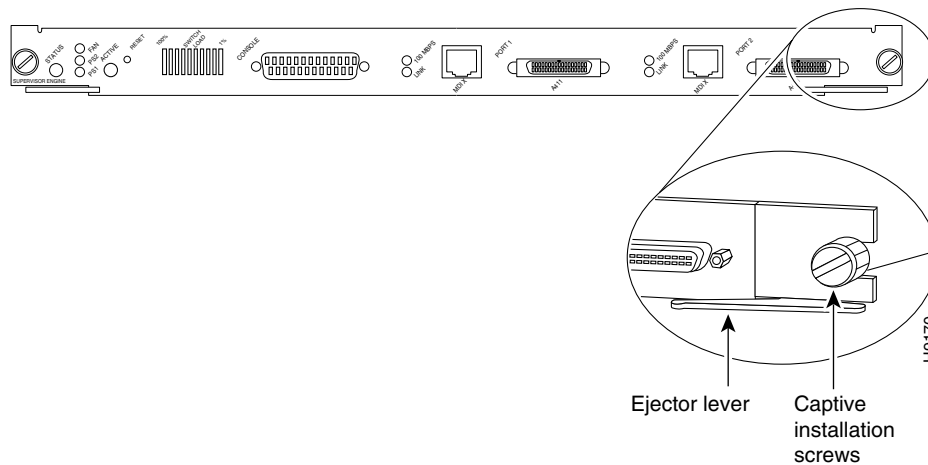
For instructions on installing and replacing switching modules, refer to the *Catalyst 5000 Series Module Installation Guide*.

Avoiding Problems When Inserting and Removing Modules

The ejector levers on the supervisor engine and switching modules align and seat the module connectors in the backplane (see Figure 7-5). Failure to use the ejector levers to insert the module can disrupt the order in which the pins make contact with the backplane. Follow the installation and removal instructions carefully.

When removing a module, use the ejector levers to ensure that the module connector pins disconnect from the backplane properly. Any supervisor engine or switching module that is only partially connected to the backplane can disrupt the system. Detailed instructions for removing and installing switching modules are described in the *Catalyst 5000 Series Module Installation Guide*.

Figure 7-5 Ejector Levers and Captive Installation Screws (Supervisor Engine II Shown)



Tools Required

Use a flat-blade screwdriver to remove any filler (blank) modules and to tighten the captive installation screws that secure the modules in their slots. When you handle modules, use an ESD-preventive wrist strap or other grounding device to prevent electrostatic discharge (ESD) damage.

Removing the Supervisor Engine

Before you remove a supervisor engine, you should first upload the current configuration to a server. This saves time when bringing the module back online. You can recover the configuration by downloading it from the server to the nonvolatile memory of the supervisor engine.

To remove a supervisor engine, perform the following steps:

- Step 1** If you do not plan to immediately reinstall the supervisor engine you are removing, disconnect any network interface cables attached to the module ports.
- Step 2** Use a screwdriver to loosen the captive installation screws at the left and right sides of the module.
- Step 3** Grasp the left and right ejector levers and simultaneously pull the left lever to the left and the right lever to the right to release the module from the backplane connector.

- Step 4** Grasp the handle of the module with one hand and place your other hand under the carrier to support and guide the module out of the slot. Avoid touching the module.
- Step 5** Carefully pull the module straight out of the slot, keeping your other hand under the carrier to guide it. Keep the module at a 90-degree orientation to the backplane.
- Step 6** Place the removed module on an antistatic mat or antistatic foam.
- Step 7** If the slot is to remain empty, install a module filler plate to keep dust out of the chassis and to maintain proper airflow through the module compartment.

**Caution**

Always install a switching module filler plate in empty switching module slots to maintain the proper flow of cooling air across the modules.

**Note**

When you remove and replace the supervisor engine, the system provides status messages on the console screen. The messages are for information only. Enter the **show system** and **show module** commands to view specific information. For additional information, refer to the *Catalyst 5000 Series Software Configuration Guide* and the *Catalyst 5000 Series Command Reference*. Also, refer to the Preface for a description of Cisco Connection Online (CCO).

Replacing the Supervisor Engine

To replace the supervisor engine, perform the following steps. Note that the supervisor engine must go in slot 1 and the redundant supervisor engine in slot 2.

- Step 1** Remove the module filler plate, if any.
- Step 2** Grasp the handle of the module with one hand and carefully align the module with the slot, keeping your other hand under the carrier to support it. Keep the module at a 90-degree orientation to the backplane.
- Step 3** Carefully push the module straight into the slot, keeping one hand under the carrier to guide it. Avoid touching the module.
- Step 4** Make sure that the ejector levers are pushed in, holding the module to the backplane connector.
- Step 5** Use a screwdriver to tighten the captive installation screws at the left and right sides of the module.
- Step 6** Reattach network interface cables to the module ports.

Using Flash Memory (PCMCIA) Cards (Supervisor Engine III)

The Flash memory (PCMCIA) card slots on the front panel of Supervisor Engine III are for additional PCMCIA-based Flash memory. You can use this Flash memory to store and run Cisco IOS images, or to serve as an I/O device. Occasionally, it might be necessary to remove and replace Flash memory cards; however, removing Flash memory cards is not required and is not recommended after the cards are installed in the slots.

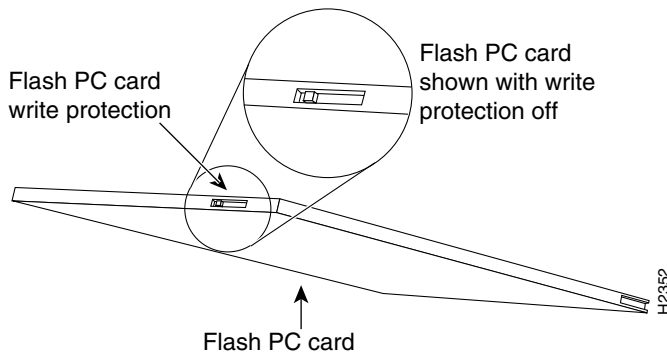
Supervisor Engine III has two PCMCIA slots: slot 0 (bottom) and slot 1 (top). The following procedure is generic and can be used for a Flash memory card in either slot position.

**Note**

You can insert and remove the Flash memory card with the power on.

Before you install a card, verify that the Flash memory card is set with write protection off. The write-protect switch is located on the front edge of the card when oriented with the printing right side up and the edge connector end away from you. (See Figure 7-6.)

Figure 7-6 Locating the Flash Memory Card Write-Protection Switch



Use the following procedure for installing and removing a Flash memory card:

-
- Step 1** Face the front panel of the switch and hold the Flash memory card with the connector end of the card toward the slot. The connector end of the card is opposite the end with the write-protection switch, which is shown in Figure 7-6.
- Step 2** Insert the card into the appropriate slot until the card completely seats in the connector at the back of the slot and the eject button pops out toward you. Note that the card does not insert all the way into the slot; a portion of the card remains outside the slot. *Do not attempt to force the card past this point.*
- Step 3** To eject a card, press the appropriate ejector button until the card is free of the connector at the back of the slot.
- Step 4** Remove the card from the slot and place it in an antistatic bag.
-

Removing and Replacing the Power Supply

This section describes the procedure you use to remove and install power supplies for the Cisco Catalyst 5500 switches. Use a flat-blade screwdriver to perform these procedures.

- Removing an AC-Input Power Supply, page 7-9
- Installing an AC-Input Power Supply, page 7-10
- Removing a DC-Input Power Supply, page 7-11
- Installing a DC-Input Power Supply, page 7-13

Removing an AC-Input Power Supply

Follow these steps to remove an AC-input power supply:



Note

In systems with redundant power supplies, the faulty supply can be replaced while the system is operating.

Step 1

Turn off the power switch on the power supply you are removing (see Figure 7-7).



Warning

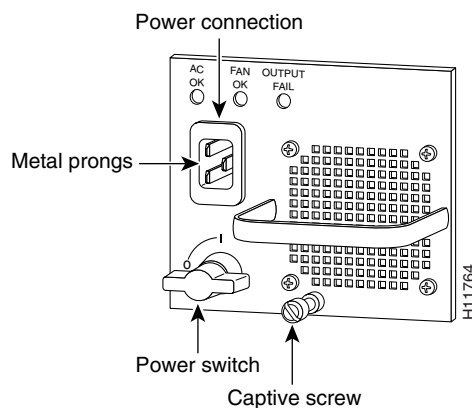
Do not touch the power supply when the power cord is connected. For systems with a power switch, line voltages are present within the power supply even when the power switch is off and the power cord is connected. For systems without a power switch, line voltages are present within the power supply when the power cord is connected.



Caution

Failure to turn off the power supply could result in equipment damage.

Figure 7-7 AC-Input Power Supply Front Panels



Step 2

Disconnect the power cord from the power source.



Warning

Before working on a chassis or working near power supplies, unplug the power cord on AC units; disconnect the power at the circuit breaker on DC units.

Step 3

Disconnect the power cord from the power supply being removed.

Step 4

Using a flat-blade screwdriver, loosen and remove the captive installation screws (see Figure 7-7).

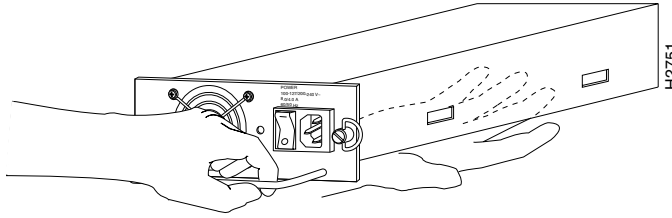


Caution

Use both hands to install and remove power supplies.

Step 5

Grasp the power supply handle with one hand and place your other hand underneath to support the bottom of the supply, as shown in Figure 7-8 (Cisco Catalyst 5000 supply shown).

Figure 7-8 Handling an AC-Input Power Supply**Warning**

Keep your hands and fingers out of the power supply bays. High current is present on the power backplane when the system is operating.

Step 6 Pull the supply out of the bay and put it aside.

Step 7 If the power supply bay is to remain empty, install a blank power supply filler plate over the opening; secure it with the mounting screws.

**Caution**

Always install a filler plate over an empty power supply bay, not only to protect the inner chassis and connectors from dust or other contamination, but to prevent possible contact with the high current levels of those connectors when the chassis is powered on.

Installing an AC-Input Power Supply

**Warning**

Before installing a Cisco Catalyst 5500 AC-input power supply, read the warning in the “Removing an AC-Input Power Supply” section.

Follow these steps to install an AC-input power supply:

Step 1 Turn off the power switch on the power supply you are installing (see Figure 7-9).

**Caution**

Failure to turn off the power supply could result in equipment damage.

**Caution**

Use both hands to install and remove power supplies. The Cisco Catalyst 5500 power supply weighs 22 lb. (9.9 kg).

**Warning**

Keep your hands and fingers out of the power supply bays. High current is present on the power backplane when the system is operating.

Step 2 Grasp the power supply handle with one hand and place your other hand underneath to support the bottom of the supply, as shown in Figure 7-11.

- Step 3** Slide the power supply all the way into the power supply bay.
- Step 4** Using a flat-blade screwdriver, tighten the captive installation screws (see Figure 7-10).
- Step 5** Before connecting the power supply to a power source, ensure that all site power and grounding requirements described in the *Cisco Media Gateway Controller Hardware Installation Guide* have been met.
- Step 6** Plug the power cord into the power supply.
- Step 7** Connect the other end of the power cord to an AC-power input source.

**Note**

Each AC-input power supply operating at 120 VAC requires a dedicated 20A service and 20A plug and receptacle. It is not acceptable to power the Cisco Catalyst 5500 from a 15A line cord because of the safety ratings under which the Cisco Catalyst 5500 is certified.

**Caution**

In a system with dual power supplies, connect each power supply to a separate input source. In case of a power source failure, the second source will probably still be available and can maintain maximum overcurrent protection for each power connection.

- Step 8** Turn the power switch to the ON position on the power supply.
- Step 9** Verify that power supply operation and the front panel LEDs are in the following states:
- AC OK LED is green.
 - FAN OK LED is green.
 - OUTPUT FAIL LED is off.
- Step 10** Verify that the appropriate supervisor engine module PS1 and PS2 LEDs are on (green).
- Step 11** Enter the **show system** command to display the power supply and system status.
- If the LEDs or **show system** command indicate a power or other system problem, refer to Appendix C, “Troubleshooting Cisco Catalyst 5500 Multiswitch Routers Signaling,” for troubleshooting information.

Removing a DC-Input Power Supply

Follow these steps to remove a DC-input power supply (product number WS-C5568):

- Step 1** Verify that power is off to the DC circuit on the power supply you are removing.

**Warning**

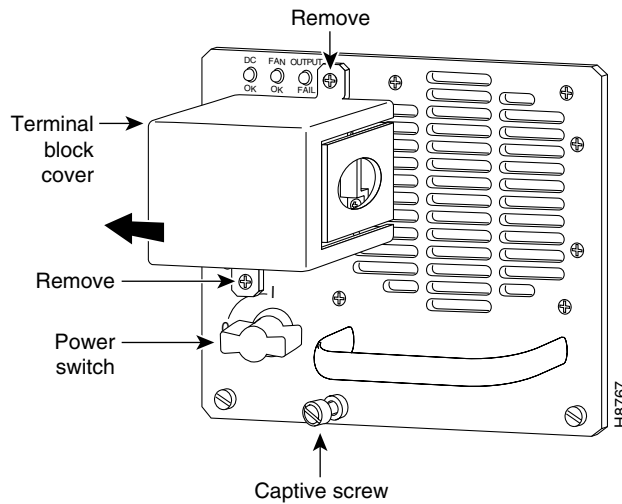
Before performing the following procedures, ensure that power is removed from the DC circuit. To ensure that all power is OFF, locate the circuit breaker on the panel board that services the DC circuit, switch the circuit breaker to the OFF position, and tape the switch handle of the circuit breaker in the OFF position.

**Warning**

Before working on a chassis or working near power supplies, unplug the power cord on AC units; disconnect the power at the circuit breaker on DC units.

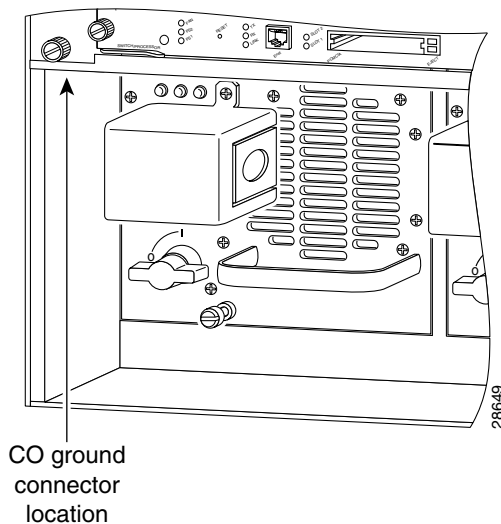
- Step 2** Turn the power switch to the OFF (0) position on the power supply you are removing (see Figure 7-9).
- Step 3** Remove the two screws securing the terminal block cover and slide the cover straight off the terminal block (see Figure 7-9).

Figure 7-9 DC-Input Power Supply Front Panels



- Step 4** Disconnect the DC-input wires from the terminal block. Disconnect the ground wire last.
- Step 5** Disconnect the central office (CO) ground from the CO ground connector (Figure 7-10).

Figure 7-10 DC-Input Power Supply CO Ground



- Step 6** Loosen and remove the captive screws on the power supply (see Figure 7-9).



Caution

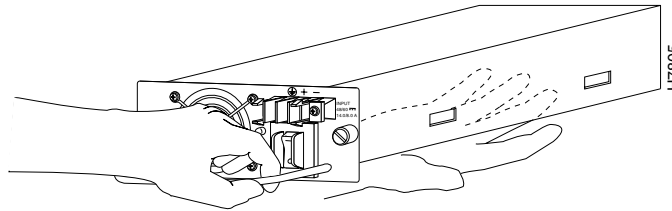
Use both hands to remove and install power supplies.

- Step 7** Grasp the power supply handle with one hand and place your other hand underneath as you slowly pull the power supply out of the bay (see Figure 7-11).

**Warning**

Keep hands and fingers out of the power supply bays. High voltage is present on the power backplane when the system is operating.

Figure 7-11 Handling a DC Power Supply



- Step 8** If the bay is to remain empty, install a blank power supply filler plate (Cisco part number 700-00177-01) over the opening and secure it with the mounting screws. This protects the inner chassis from dust and prevents accidental contact with live voltage at rear of the bay.

**Caution**

Always install a filler plate over an empty power supply bay to protect the inner chassis and connectors from dust or other contamination and to prevent possible contact with the high current levels of those connectors when the chassis is powered on.

- Step 9** Reinstall the power supply terminal block cover.

Installing a DC-Input Power Supply

Follow these steps to install a DC-input power supply:

- Step 1** Verify that power is off to the DC circuit on the power supply you are installing.

**Warning**

Before performing any of the following procedures, ensure that power is removed from the DC circuit. To ensure that all power is OFF, locate the circuit breaker on the panel board that services the DC circuit, switch the circuit breaker to the OFF position, and tape the switch handle of the circuit breaker in the OFF position.

**Warning**

Before working on a chassis or working near power supplies, unplug the power cord on AC units; disconnect the power at the circuit breaker on DC units.

- Step 2** Connect the switch to the CO ground through the CO ground connector shown in Figure 7-10. Remove the adhesive strip covering the CO ground connector on the switch.

Use the following guidelines when connecting the switch to the CO ground:

- The ground wire lug must be less than or equal to 0.320 in. (8.1 mm) to fit within the ground connector.

- The ground wire must be 10 to 12 AWG. Use the larger gauge ground wire when the switch is further away from the ground location.

Step 3 Turn the power switch to the OFF (0) position on the power supply you are installing (see Figure 7-10).

**Caution**

Use both hands to remove and install power supplies.

**Warning**

Keep hands and fingers out of the power supply bays. High voltage is present on the power backplane when the system is operating.

Step 4 Grasp the power supply handle with one hand and place your other hand underneath as you slowly insert the power supply into the bay (see Figure 7-11).

Step 5 Using a screwdriver, tighten the captive screws on the power supply (see Figure 7-9).

Step 6 Remove the terminal block cover (see Figure 7-9). Remove the two screws securing the terminal block cover and slide the cover straight off the terminal block.

Step 7 Attach the appropriate lugs to the DC-input wires. Maximum width of the lugs is 0.300 inch (7.6 mm). Suggested lugs are AMP 322985 or 52941. Suggested DC-input wires are 10 AWG.

**Caution**

When stranded wiring is required, use approved wiring terminations, such as closed-loop or spade-type with upturned lugs. These terminations must be the appropriate size for the wires and clamp both the insulation and conductor.

Step 8 Connect the DC-input wires to the terminal block.

If not already done, route the DC-input power cable through the conduit from your power source, through the conduit bracket on the power supply, and make a sufficient length of wire available to attach to the three terminal block connections.

Attach and tighten the conduit to the conduit bracket. How this conduit is attached depends on your site; its attachment is beyond the scope of this document.

**Caution**

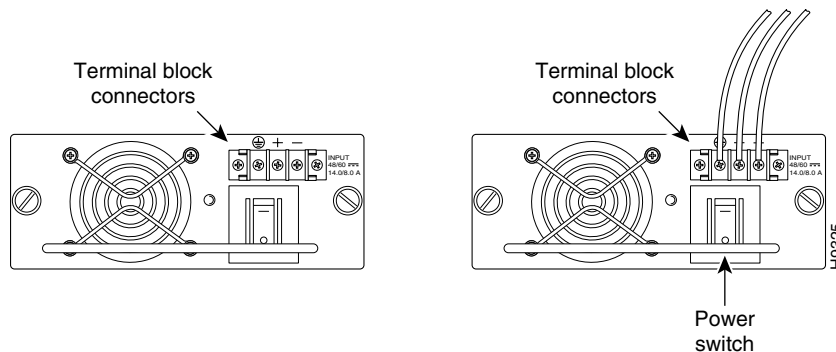
Connect the ground wire *first*.

Step 9 Connect the DC-input wires to the terminal block (see Figure 7-12). The proper wiring sequence is ground to ground, positive to positive (line to L), and negative to negative (neutral to N). Note that the ground wire should always be connected first and disconnected last.

Step 10 After ensuring that all wire connections are secure, reinstall the terminal block cover.

**Caution**

To prevent a short-circuit or shock hazard after wiring the DC-input power supply, reinstall the terminal block cover.

Figure 7-12 DC-Input Power Supply Connectors**Caution**

In a system with dual power supplies, use the modular power cord to connect each power supply to a separate input line. In case of a line failure, the second source will most likely still be available and can maintain maximum overcurrent protection for each power connection.

Step 11 Remove the tape from the circuit breaker switch handle and restore power by moving the circuit breaker switch handle to the on position.

Step 12 Turn the power switch to the on position on the power supply.

Step 13 Verify power supply operation.

Verify that the power supply front panel LEDs are in the following states:

DC OK LED is green.

FAN OK LED is green.

OUTPUT FAIL LED is off.

Verify that the appropriate supervisor engine module PS1 and PS2 LEDs are on and green.

Enter the **show system** command to display the power supply and system status.

Removing and Replacing the Chassis Fan Assembly

This section describes how to remove and install chassis fan assemblies. Use a flat-blade screwdriver to perform this procedure.

Removing the Fan Assembly

Perform the following steps to remove the existing chassis fan assembly:

**Caution**

Never operate the system if the fan assembly is removed or if it is not functioning properly. An overtemperature condition can result in severe equipment damage.

**Note**

The fan assembly is designed to be removed and replaced while the system is operating without presenting an electrical hazard or damage to the system.

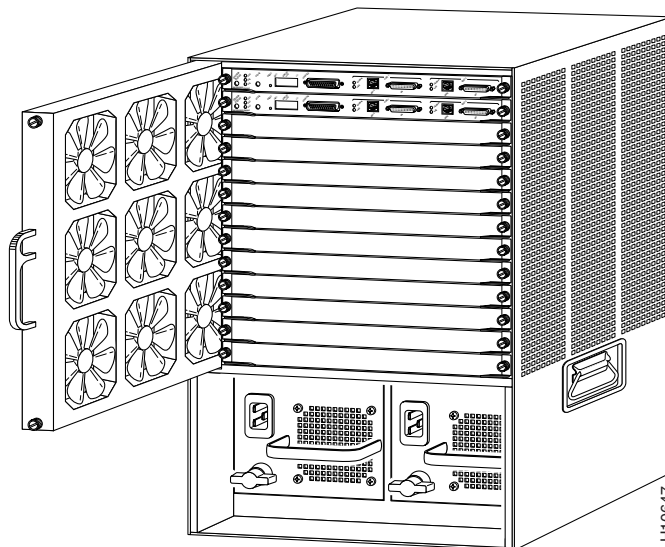
-
- Step 1** Locate the fan assembly to the left of the card cage (see Figure 7-13).
- Step 2** Loosen the two captive installation screws by turning them counterclockwise.
- Step 3** Grasp the fan assembly with both hands and pull it outward, joggling it if necessary to unseat it from the backplane. Pull it clear of the chassis and place it in a safe location.
-

Installing the Fan Assembly

Perform the following steps to install the new fan assembly:

-
- Step 1** Hold the fan assembly with the fans facing to the right.
- Step 2** Place the fan assembly into the front chassis cavity so that it rests on the chassis, and then lift the fan assembly up slightly, aligning the top and bottom guides.
- Step 3** Push the fan assembly into the chassis until the captive installation screws meet the chassis.
- Step 4** Tighten the captive installation screws by turning them clockwise.
-

Figure 7-13 Cisco Catalyst 5500 Chassis Fan Assembly



Checking the Installation

Perform the following steps to verify that the new fan assembly is installed correctly:

-
- | | |
|---------------|--|
| Step 1 | Listen for the fans; you should immediately hear them operating. If you do not hear them, ensure that the fan assembly is completely inserted in the chassis and that the faceplate is flush with the switch back panel. |
| Step 2 | If after several attempts the fans do not operate, or if you experience trouble with the installation (for instance, if the captive installation screws do not align with the chassis holes), contact the Cisco Technical Assistance Center (TAC) for assistance. Refer to the “Obtaining Technical Assistance” section on page xviii for information on contacting the Cisco TAC. |
-



Troubleshooting the Cisco MGC Node

This chapter describes troubleshooting methods for the Cisco Media Gateway Controller (MGC) node. It includes the following sections to help you isolate system problems:

- Troubleshooting Overview, page 8-1
- Troubleshooting Using Cisco MGC Alarms, page 8-2
- SS7 Network Related Problems, page 8-50
- Bearer Channel Connection Problems, page 8-69
- Tracing, page 8-102
- Platform Troubleshooting, page 8-112

Troubleshooting Overview

This chapter uses the alarms and logs that appear at the Cisco MGC as the basis for isolating problems within the system. You can find a complete listing of alarms and logs in the *Cisco Media Gateway Controller Software Release 7 Messages Reference Guide*.

Typically, suggested corrective actions start with simple troubleshooting tasks and become increasingly more complex. It is easier, for example, to check LEDs and cabling than to perform a call trace. The suggested corrective actions point to other chapters in this manual, as well as to troubleshooting tools including the Cisco MGC software, the Cisco WAN Manager, and CiscoWorks.

Additionally, you will find examples of troubleshooting typical problems. The examples provide a logical sequence for troubleshooting that you can use as a model.



Note

Troubleshooting of the Cisco MGC node should be performed by someone who has been trained in the complexities of the system, who has some experience administering the system, and who understands UNIX at the system administrator level.

The following sections contain various equipment failure scenarios for the solution, including

- Cisco SLT Failure
- Cisco MGC Failure
- Operating System Failure

Cisco SLT Failure

Each Cisco Signaling Link Terminal (SLT) has an Reliable User Datagram Protocol (RUDP)/User Datagram Protocol (UDP)/IP connection to each Cisco MGC for the transfer of Message Transfer Part (MTP) Level 3 (MTP3), ISDN User Part (ISUP), and Transaction Capabilities Application Part (TCAP) information. A Cisco SLT platform failure results in the surviving Cisco SLT platforms taking over the distribution of messages to the active Cisco MGC. Cisco SLT platforms should be provisioned so that half of the platforms can support the entire signaling load. The result is that a Cisco SLT platform failure has no significant effect on call processing.

There are several Cisco SLT failure scenarios to consider:

- An IP link failure between the Cisco SLT and the Cisco MGC, which indicates that it is impossible to transfer MTP3 messages. In this case, MTP Level 2 (MTP2) transmits Status Indication Processor Outage (SIPO) messages to the signaling transfer point (STP) to initiate switchover to another Cisco SLT.
- In the case where MTP2 failed (equivalent to a Cisco SLT failure), no SIPO messages are sent because MTP2 is inoperable. Instead, the mated STP pair detects the failure because of timer expiration or link unavailability and initiates the switchover to another SS7 link.
- If a Cisco MGC fault is detected by a Cisco SLT timer, a coordination mechanism causes SS7 messaging to flow to the newly active (formerly standby) Cisco MGC. The standby Cisco MGC assumes control for all calls in progress and all new calls.

Cisco MGC Failure

Cisco MGC hosts run in active-standby mode. The call-processing application is active on only one Cisco MGC platform at a time, and the application switches to the standby platform when a critical alarm occurs. The result is that Cisco MGC failure and switchover events are invisible to the SS7 signaling network.

Cisco MGC alarms can be configured as minor, major, or critical. Critical alarms are generated whenever any significant failure occurs. Any critical alarm causes a switchover to occur. For example, if the call engine or I/O channel controller (IOCC)-MTP in the active Cisco MGC should fail, there is a disconnection from the process manager and a switchover to the standby Cisco MGC.

Operating System Failure

An operating system (OS) or hardware failure in the active Cisco MGC can also cause a switchover to the standby Cisco MGC. The failover daemon in the standby Cisco MGC detects the failure of the active Cisco MGC and instructs the process manager to initiate a switchover. The standby Cisco MGC then takes over all call-processing functions. The switchover is transparent to all the Cisco SLTs.

Troubleshooting Using Cisco MGC Alarms

The Cisco MGC generates alarms to indicate problems with processes, routes, linksets, signaling links, and bearer channels. The *Cisco Media Gateway Controller Software Release 7 Messages Reference Guide* lists all of the Cisco MGC alarms and logs, and provides descriptions, possible causes, and suggested actions. You can find procedures for alarms that require you to take corrective action in the “Alarm Troubleshooting Procedures” section on page 8-8.

The active alarm log files reside in the /opt/CiscoMGC/var/log directory. These alarm log files are archived based on the criteria set in the dmprSink.dat file. For more information on the dmprSink.dat file, refer to the “Configuring the Data Dumper” section on page A-2.

Troubleshooting using Cisco MGC alarms is described in the following sections:

- Retrieving All Active Alarms, page 8-3
- Acknowledging Alarms, page 8-3
- Clearing Alarms, page 8-4
- Troubleshooting with System Logs, page 8-4
- Alarm Troubleshooting Procedures, page 8-8

Retrieving All Active Alarms

To retrieve all active alarms, log in to the active Cisco MGC, start a Man-Machine Language (MML) session, and enter the following command:

```
rtrv-alm
```

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"
```

Acknowledging Alarms

Acknowledging an alarm does not clear the alarm. You can still retrieve it with the **rtrv-alm** MML command. To acknowledge an alarm, log in to the active Cisco MGC, start an MML session, and enter the following command:

```
ack-alm:comp:"alarmCategory"
```

Where:

- *comp*—The MML name of the component. A complete list of components can be found in the *Cisco Media Gateway Controller Software Release 7 Provisioning Guide*. You can retrieve a list of system components by entering the **rtrv-cfg:components** MML command.
- *alarmCategory*—MML name of the associated alarm category. The entered name must match exactly the name of the alarm as it is displayed.

For example, to acknowledge a signaling channel fail alarm (SC FAIL) that occurred on the link MGC2alink1, enter the following command:

```
ack-alm:MGC2alink1:"SC FAIL"
```

Clearing Alarms

You can clear an alarm for a affected component. Clearing the alarm removes it and any associated alarms from the internal processes list maintained by the Cisco MGC. To clear an alarm, log in to the active Cisco MGC, start an MML session, and enter the following command:

```
clr-alm: comp:"alarmCategory"
```

Where:

- *comp*—The MML name of the component. A complete list of components can be found in the *Cisco Media Gateway Controller Software Release 7 Provisioning Guide*. You can retrieve a list of system components by entering the **rtrv-cfg:components** MML command.
- *alarmCategory*—MML name of the associated alarm category. The entered name must match exactly the name of the alarm as it is displayed.

For example, to acknowledge a signaling channel fail alarm (SC FAIL) that occurred on the link MGC2alink1, enter the following command:

```
clr-alm:MGC2alink1:"SC FAIL"
```

Troubleshooting with System Logs

You can use system logs in conjunction with alarms to provide vital information that you can use in troubleshooting problems. A complete listing of system logs can be found in the *Cisco Media Gateway Controller Software Release 7 Messages Reference Guide*.

The active system log files reside in the /opt/CiscoMGC/var/log directory. These system log files are archived based on the criteria set in the dmprSink.dat file. For more information on the dmprSink.dat file, refer to the “Configuring the Data Dumper” section on page A-2.



Note

Log level and destination can be controlled through settings in the XECfgParm.dat file. Refer to the *Cisco Media Gateway Controller Software Release 7 Installation and Configuration Guide* for more information.

Viewing System Logs

The best method to use to view logs is to use the log viewer, which is part of the Cisco MGC viewer toolkit. The log viewer enables you to search for specific log information, accounts for log rotations, and makes new logs available. The log server is responsible for log rotation. The log server closes the current file, and creates a new file for current logging. The log viewer also has an option for exporting the results of a log file search to a UNIX file.

For more information on using the log viewer, refer to the “Using the Log Viewer” section on page 3-114.

To view a log file when you do not have the Cisco MGC viewer toolkit installed on your system, complete the following steps:

Step 1 Log in to the active Cisco MGC enter the following UNIX command to change to the /opt/CiscoMGC/var/log directory:

```
cd /opt/CiscoMGC/var/log
```

Step 2 Enter the following UNIX command to list the available logs:

```
ls
```

The system returns a response similar to the following:

```
alm.csv                platform.log
cdr.bin                platform_20010516141831.log
meas.csv               platform_20010517040508.log
mml.log               platform_20010518040508.log
mml_20010516141831.log platform_20010519040508.log
mml_20010517040508.log platform_20010520040508.log
mml_20010518040508.log platform_20010521040508.log
```

Step 3 To view a specific system log file, enter the following command:

```
cat log_file_name | more
```

Where *log_file_name* is the name of the log file you want to view.



Note

Because the log files are very large, use the more parameter to scroll through the file. You might prefer to print the file to find the information you need.

For example, you would enter the following command to view a specific platform log file:

```
cat platform_20010516141831.log | more
```

The system returns a response similar to the following:

```
Tue May  8 13:35:32:920 2001 | cdrDmpr (PID 15526) <Error>
GEN_ERR_GETCFGPARAM: cdrDmprSink::readObj: Failed to get MGC_CDR_NODE_ID for facility *

Tue May  8 13:35:32:921 2001 | cdrDmpr (PID 15526) <Error>
GEN_ERR_GETCFGPARAM: cdrDmprSink::readObj: Failed to get MGC_CDR_NODE_ID for facility *

Tue May  8 13:35:32:922 2001 | cdrDmpr (PID 15526) <Error>
GEN_ERR_GETCFGPARAM: cdrDmprSink::readObj: Failed to get MGC_CDR_NODE_ID for facility
*Process id is 15517 and thead id is 1 in set the destination

Tue May  8 13:37:13:201 2001 | unknown (PID 15663) <Info>
/tmp/almM_input: installed time handler, hdlrId = 1

Tue May  8 13:37:31:786 2001 | engine (PID 15590) <Error>
CP_ERR_START_GWAY_AUDIT: engProcEvtHdlr::handleGoActiveLocal Failed to start GWAY
auditProcess id is 15508 and thead id is 1 in set the destination
Process id is 15509 and thead id is 1 in set the destination

--More--
```

Understanding System Log Messages

Each system log message uses the following format:

Timestamp, Process Name, Process ID, <Log Level>, Log ID:<Message Text>

- **Timestamp**—Displays the date and time on the system when the log message was created, for example, “May 8 01:35:23:047 2001”. The time displayed is down to the millisecond level.
- **Process Name**—Displays the name of the process that created the log message, for example, “engine”.
- **Process ID**—Displays the identification number of the process that created the log message, for example, “(PID29974)”.
- **Log Level**—Displays the severity level of the log message, for example, “Info”.
- **Log ID**—Displays a short, symbolic name for the message, for example, “GEN_ERR_GETCFGPARAM”.
- **Message Text**—Displays the log message text, for example, “installed time handler, hdlrId = 1”. The message text can take up multiple lines, but is typically only a single line.

Changing the Log Level for Processes

In order to control the types of log messages being written to the system log file, you can use the **set-log** MML command to change the logging level for system processes. The Cisco MGC can generate a large number of logged events, which can result in large numbers of archived system log files in the `opt/CiscoMGC/var/spool` directory. For example, if the `maxTime` parameter in the `dmprSink.dat` file is set to 15 minutes, over 2000 files are created in the `opt/CiscoMGC/var/spool` directory daily. Therefore, you might want to limit the number of logs being created by changing the logging level of the Cisco MGC software processes.

Table 8-1 lists the logging levels that can be selected for the Cisco MGC software processes without severely degrading system performance.

Table 8-1 Processes and their Lowest Possible Logging Levels

| Process | Lowest Logging Level Without Severe Performance Degradation |
|------------|--|
| Engine | Informational (the debug level causes major performance impacts—do not set). |
| All others | Debug, but only a single process can be in debug at any point in time. |



Caution

Debug level logging provides extremely verbose output and, if misused, can cause severe system performance degradation.

To change the log level of a single process, log in to the active Cisco MGC, start an MML session, and enter the following command:

```
set-log:process_name:log_level[,confirm]
```

Where:

- **process_name**—Name of the process for which you want to change the logging level. Processes are listed in the “Understanding Processes” section on page 3-4.

- *log_level*—Desired logging level. Valid log levels are as follows:
 - CRIT—Critical level messages
 - WARN—Warning condition messages
 - ERR—Error condition messages
 - TRACE—Trace messages
 - INFO—Informational messages
 - DEBUG—Debug-level messages (lowest level). Do not set the process to this logging level unless directed to do so by the Cisco Technical Assistance Center (TAC).
- **confirm**—Used when changing the logging level of a process to debug (DEBUG).

**Note**

Setting the logging level at a given level means that the information related to the levels above the selected level are included. In other words, setting a process to the INFO logging level means that information related to the TRACE, ERR, WARN, and CRIT levels are also displayed. The order of the levels shown above can also be viewed as a verbosity level, in that at CRIT, the least information is logged and at DEBUG the most information logged.

For example, to change the log level of the engine, enter the following command:

```
set-log:eng-01:info
```

To change the log level of all processes, log in to the active Cisco MGC, start an MML session, and enter the following command:

```
set-log:all:log_level
```

Where *log_level* is the desired logging level. Valid log levels are as follows:

- CRIT—Critical level messages
- WARN—Warning condition messages
- ERR—Error condition messages
- TRACE—Trace messages
- INFO—Informational messages

**Note**

Setting the logging level at a given level means that the information related to the levels above the selected level are included. In other words, setting a process to the INFO logging level means that information related to the TRACE, ERR, WARN, and CRIT levels are also displayed. The order of the levels shown above can also be viewed as a verbosity level, in that at CRIT, the least information is logged and at DEBUG the most information logged.

For example, to change the log level of all processes to warning, enter the command:

```
set-log:all:warn
```

**Note**

The logging level of the process manager (PM-01) cannot be set using the **set-log:all:log_level** MML command. You can only change the logging level of the process manager using the **set-log:pm-01:log_level** MML command.

**Note**

The **set-log:all:log_level** MML command cannot be used to set all of the processes to the debug (DEBUG) logging level.

**Note**

The disk monitor (DSKM-01) process does not accept log-level change requests.

Creating a Diagnostics Log File

You can create a diagnostics log file that records the MML commands and responses that you execute. To do this, perform the following steps:

-
- Step 1** Create a diagnostics log file by logging in to the active Cisco MGC, starting an MML session, and entering the following command:
- Step 2** Perform your troubleshooting procedures.
- Step 3** When you have finished troubleshooting and you want to view your diagnostics file, enter the following command at the active Cisco MGC:

```
diaglog:filename:start
```

Where *filename* is the name of your diagnostics log file. Enter the name only, do not enter a suffix, such as .log.

```
diaglog:filename:stop
```

The file, which is given the name you entered in Step 1, without a suffix, can be found in the \$BASEDIR/var/log directory. You can view the file using a text editor, such as vi.

Alarm Troubleshooting Procedures

This section contains alarms that require you to take corrective action. A complete list of alarms, including those that do not require you to take corrective action, can be found in the *Cisco Media Gateway Controller Software Release 7 Messages Reference Guide*.

All Conn Cntl Links Fail

This alarm occurs when the MGCP/SRCP session loses a heartbeat, indicating that the session is down.

Corrective Action

To correct the problem identified by this alarm, perform the following steps:

-
- Step 1** Verify that the Ethernet interfaces between the Cisco MGC and the associated media gateway are working properly.

**Note**

Information on verifying the proper operation of an Ethernet interface on the Cisco MGC host can be found in the Sun Microsystems documentation that came with your system. Information on verifying the proper functioning of an Ethernet interface on the media gateway can be found in its associated documentation.

If an element of the Ethernet connection (such as a cable or an Ethernet interface card) is not working properly, replace it. Otherwise, proceed to Step 2.

**Note**

Information on removing and replacing an Ethernet interface card on the Cisco MGC host can be found in the Sun Microsystems documentation that came with your system. Information on removing and replacing an Ethernet interface card on the media gateway can be found in its associated documentation.

- Step 2** Verify that the near-end and far-end MGCP/SRCP sessions are operating normally. Refer to the documentation for the affected media gateway for more information on verifying the functioning of the MGCP/SRCP sessions.

If the MGCP/SRCP sessions are not operating normally, return the MGCP/SRCP sessions to normal operations, as described in the documentation for the affected media gateway. Otherwise, proceed to Step 3.

- Step 3** Contact the Cisco TAC to further analyze the problem and determine a solution. For more information about contacting the Cisco TAC, refer to the “Obtaining Technical Assistance” section on page xviii.

All C7 IP Links Fail

This alarm occurs when communication is lost to all Cisco SLTs of a single protocol family. This defaults to a critical alarm, and causes an automatic switchover, if a standby Cisco MGC is present.

Corrective Action

To correct the problem identified by this alarm, perform the following steps:

- Step 1** Verify that the Cisco SLTs are operating normally, as described in the “Checking Equipment Status” section on page 6-2 and the “Using the Cisco SLT Operating System to Check Status” section on page 6-4.
- Step 2** Verify that the Ethernet interfaces between the Cisco MGC and the Cisco SLTs are working properly.

**Note**

Information on verifying the proper operation of an Ethernet interface on the Cisco MGC host can be found in the Sun Microsystems documentation that came with your system. Information on verifying the proper functioning of an Ethernet interface on the Cisco SLT can be found in the “Checking Equipment Status” section on page 6-2 and the “Using the Cisco SLT Operating System to Check Status” section on page 6-4.

If an element of the Ethernet connection (such as a cable or an Ethernet interface card) is not working properly, replace it. Otherwise, proceed to Step 2.



Note

Information on removing and replacing an Ethernet interface card on the Cisco MGC host can be found in the Sun Microsystems documentation that came with your system. Information on removing and replacing an interface card on the Cisco SLT can be found in the “Replacing Hardware Components” section on page 6-13.

- Step 3** Verify that the configuration for your system is correct. To verify the provisioning data for your Cisco MGC, use the **prov-rtrv** MML command, as described in the “Retrieving Provisioning Data” section on page 3-67. To verify the provisioning data for the Cisco SLTs, use show commands, as described in the “Using the Cisco SLT Operating System to Check Status” section on page 6-4.
- If the configuration of your Cisco MGC is incorrect, begin a dynamic reconfiguration session, as described in the “Invoking Dynamic Reconfiguration” section on page 3-65.
- If the configuration of your Cisco SLTs is incorrect, modify the provisioning data for your system. Refer to the *Cisco Signaling Link Terminal document* for more information.
- If the configuration of both the Cisco MGC and the Cisco SLTs are correct, then proceed to Step 4.
- Step 4** Contact the Cisco TAC to further analyze the problem and determine a solution. For more information about contacting the Cisco TAC, refer to the “Obtaining Technical Assistance” section on page xviii.

All ISDN IP Conn Fail

This alarm occurs when communication is lost to all access servers. This alarm causes an automatic switchover, if a standby Cisco MGC is present.

Corrective Action

To correct the problem identified by this alarm, perform the following steps:

- Step 1** Verify that the affected media gateways are operating normally, as described in the associated documentation.
- Step 2** Verify that the Ethernet interfaces between the Cisco MGC and the media gateways are working properly.



Note

Information on verifying the proper operation of an Ethernet interface on the Cisco MGC host can be found in the Sun Microsystems documentation that came with your system. Information on verifying the proper functioning of an Ethernet interface on a media gateway can be found in its associated documentation.

If an element of the Ethernet connection (such as a cable or an Ethernet interface card) is not working properly, replace it. Otherwise, proceed to Step 2.



Note

Information on removing and replacing an Ethernet interface card on the Cisco MGC host can be found in the Sun Microsystems documentation that came with your system. Information on removing and replacing an Ethernet interface card on the media gateway can be found in its associated documentation.

- Step 3** Verify that the configuration for your system is correct. To verify the provisioning data for your Cisco MGC, use the **prov-rtrv** MML command, as described in the “Retrieving Provisioning Data” section on page 3-67. To verify the provisioning data for the media gateways, use show commands, as described in the associated documentation.
- If the configuration of your Cisco MGC is incorrect, begin a dynamic reconfiguration session, as described in the “Invoking Dynamic Reconfiguration” section on page 3-65.
- If the configuration of your media gateways is incorrect, modify the provisioning data for the media gateways. Refer to the documentation associated with the media gateway for more information.
- If the configuration of the Cisco MGC and the media gateways are correct, then proceed to Step 4.
- Step 4** Contact the Cisco TAC to further analyze the problem and determine a solution. For more information about contacting the Cisco TAC, refer to the “Obtaining Technical Assistance” section on page xviii.
-

ANAL: ALoopCtrExceeded

This alarm occurs when an A-number analysis operation has gone into an infinite loop. The purpose of the alarm is to limit the number of passes spent in the analysis tree to 30.

Corrective Action

To correct the problem identified by this alarm, perform the following steps:

- Step 1** Validate that there are no infinite loops in the A-number dial plan, as described in the “Verifying a Dial Plan Translation” section on page 3-118.
- If there are infinite loops in your A-number dial plan, modify the settings in your A-number dial plan to remove the infinite loops, using the **numan-ed** MML command and reload the dial plan file, using the **chg-dpl** MML command. Refer to the *Cisco Media Gateway Controller Software Release 7 Dial Plan Guide* for more information.
- If there are no infinite loops in your A-number dial plan, then proceed to Step 2.
- Step 2** Contact the Cisco TAC to further analyze the problem and determine a solution. For more information about contacting the Cisco TAC, refer to the “Obtaining Technical Assistance” section on page xviii.
-

ANAL: ATableFail_GetDigTree

This alarm occurs when an invalid path for A-number analysis has been given or that the A-number analysis table is not loaded. The problem is caused when an invalid path has been specified for A-number analysis or the A-number analysis table is not loaded.

Corrective Action

To correct the problem identified by this alarm, verify that the dial plan file was loaded correctly, using the procedure described in “Verifying Proper Loading of a Dial Plan” section on page 8-69.

ANAL: ATableFail_GetDigMod

This alarm occurs when a retrieval of a modification string failed during A-number analysis. The problem occurs when the modification table is not loaded or a pointer to a nonexistent location in the modification table is given.

Corrective Action

To correct the problem identified by this alarm, verify that the dial plan file was loaded correctly, using the procedure described in “Verifying Proper Loading of a Dial Plan” section on page 8-69.

ANAL: ATableFail_GetResult

This alarm occurs when access to the result table failed during A-number analysis. The problem occurs if the result table is not loaded or a pointer to a nonexistent location in the result table is given.

Corrective Action

To correct the problem identified by this alarm, verify that the dial plan file was loaded correctly, using the procedure described in “Verifying Proper Loading of a Dial Plan” section on page 8-69.

ANAL: BLoopCtrExceeded

The alarm occurs when a B-number analysis operation has gone into an infinite loop. The purpose of the alarm is to limit the number of passes spent in the analysis tree to 30.

Corrective Action

To correct the problem identified by this alarm, perform the following steps:

-
- | | |
|---------------|---|
| Step 1 | <p>Validate that there are no infinite loops in the B-number dial plan, as described in the “Verifying a Dial Plan Translation” section on page 3-118.</p> <p>If there are infinite loops in your B-number dial plan, modify the settings in your B-number dial plan to remove the infinite loops, using the numan-ed MML command and reload the dial plan file, using the chg-dpl MML command. Refer to the <i>Cisco Media Gateway Controller Software Release 7 Dial Plan Guide</i> for more information.</p> <p>If there are no infinite loops in your B-number dial plan, then proceed to Step 2.</p> |
| Step 2 | <p>Contact the Cisco TAC to further analyze the problem and determine a solution. For more information about contacting the Cisco TAC, refer to the “Obtaining Technical Assistance” section on page xviii.</p> |
-

ANAL: BNum_GetFail_SrvTbl

This alarm occurs during B-number analysis when a screening result is encountered and an attempt to read the service table to determine the name of the service performing the screening fails. This is due to corruption of either the result table or the service table.

Corrective Action

To correct the problem identified by this alarm, verify that the dial plan file was loaded correctly, using the procedure described in “Verifying Proper Loading of a Dial Plan” section on page 8-69.

ANAL: BNum_MdfyBFail_AnnounceID

This alarm occurs during B-number analysis when an announcement result is encountered and analysis is unable to replace the last 4 digits of the B-number with the announcement ID. This is commonly caused by an out-of-range announcement Id (it should be 0-9999) or a B-number less than 4 digits long.

Corrective Action

To correct the problem identified by this alarm, perform the following steps:

-
- | | |
|---------------|---|
| Step 1 | Verify that all of the configured announcement IDs are within the range 0 through 9999, using the numan-rtrv MML command. Refer to the <i>Cisco Media Gateway Controller Software Release 7 Dial Plan Guide</i> for more information.

If any of the announcement IDs are outside of the range, modify its value using the numan-ed MML command and reload the dial plan file using the chg-dpl MML command. Refer to the <i>Cisco Media Gateway Controller Software Release 7 Dial Plan Guide</i> for more information. Otherwise, proceed to Step 2. |
| Step 2 | Verify that the dial plan file was loaded correctly, using the procedure described in “Verifying Proper Loading of a Dial Plan” section on page 8-69. |
-

ANAL: BTableFail_GetDigTree

This alarm occurs when an invalid path for B-number analysis has been given or that the B-number analysis table is not loaded. The problem occurs when an invalid path has been specified for B-number analysis or the B-number analysis table is not loaded.

Corrective Action

To correct the problem identified by this alarm, verify that the dial plan file was loaded correctly, using the procedure described in “Verifying Proper Loading of a Dial Plan” section on page 8-69.

ANAL: BTableFail_GetDigMod

This alarm occurs when retrieval of a modification string failed during B-number analysis. The problem occurs if the modification table is not loaded or a pointer to a nonexistent location in the modification table is given.

Corrective Action

To correct the problem identified by this alarm, verify that the dial plan file was loaded correctly, using the procedure described in “Verifying Proper Loading of a Dial Plan” section on page 8-69.

ANAL: BTableFail_GetResult

This alarm occurs when access to the result table failed during B-number analysis. The problem occurs if the result table is not loaded or a pointer to a nonexistent location in the result table is given.

Corrective Action

To correct the problem identified by this alarm, verify that the dial plan file was loaded correctly, using the procedure described in “Verifying Proper Loading of a Dial Plan” section on page 8-69.

ANAL: Cause_GetFail_CauseTbl

This alarm occurs during cause analysis when the cause table is unreadable. This can be due to the cause table being corrupted, a failure in the underlying software, or the cause table being built without all the existing call context cause values.

Corrective Action

-
- | | |
|---------------|---|
| Step 1 | Verify that the associated cause table contains all of the existing call context cause values, using the numan-rtrv MML command. Refer to the <i>Cisco Media Gateway Controller Software Release 7 Dial Plan Guide</i> for more information.

If the cause table is incomplete, modify its value using the numan-ed MML command and reload the dial plan file using the chg-dpl MML command. Refer to the <i>Cisco Media Gateway Controller Software Release 7 Dial Plan Guide</i> for more information. Otherwise, proceed to Step 2. |
| Step 2 | Verify that the dial plan file was loaded correctly, using the procedure described in “Verifying Proper Loading of a Dial Plan” section on page 8-69. |
-

ANAL: Cause_GetFail_DigModTbl

This alarm occurs during cause analysis when a B-number modification result is encountered and the digit modification string is unreadable. This can be due to the digit modification table being corrupted or an incorrect digit modification index being stored in the B-number modification result's data.

Corrective Action

-
- | | |
|---------------|---|
| Step 1 | Verify that the associated B-number digit modification table is correct, using the numan-rtrv MML command. Refer to the <i>Cisco Media Gateway Controller Software Release 7 Dial Plan Guide</i> for more information.

If the information in the B-number digit modification table is incorrect, modify its value using the numan-ed MML command and reload the dial plan file using the chg-dpl MML command. Refer to the <i>Cisco Media Gateway Controller Software Release 7 Dial Plan Guide</i> for more information. Otherwise, proceed to Step 2. |
| Step 2 | Verify that the dial plan file was loaded correctly, using the procedure described in “Verifying Proper Loading of a Dial Plan” section on page 8-69. |
-

ANAL: Cause_GetFail_InvldRsltType

This alarm occurs during cause analysis when a result is encountered that is not supported in cause analysis. This is due to corruption of the cause or location tables or the result table.

Corrective Action

To correct the problem identified by this alarm, verify that the dial plan file was loaded correctly, using the procedure described in “Verifying Proper Loading of a Dial Plan” section on page 8-69.

ANAL:Cause_GetFail_LocTbl

This alarm occurs during cause analysis when the location table is unreadable. This can be due to the location table being corrupted, a failure in the underlying software, or the location table not being fully populated with all possible references from the cause table.

Corrective Action

-
- Step 1** Verify that the associated location table contains all of the possible references from the cause table, using the **numan-rtrv** MML command. Refer to the *Cisco Media Gateway Controller Software Release 7 Dial Plan Guide* for more information.
- If the location table does not contain all of the references, modify its value using the **numan-ed** MML command and reload the dial plan file using the **chg-dpl** MML command. Refer to the *Cisco Media Gateway Controller Software Release 7 Dial Plan Guide* for more information. Otherwise, proceed to Step 2.
- Step 2** Verify that the dial plan file was loaded correctly, using the procedure described in “Verifying Proper Loading of a Dial Plan” section on page 8-69.
-

ANAL:Cause_GetFail_RsltTbl

This alarm occurs during cause analysis when the result table is unreadable. This can be due to the result table being corrupted, a failure in the underlying software, or the result table not being fully populated with all possible references from the cause and location tables.

Corrective Action

-
- Step 1** Verify that the associated result table contains all of the possible references from the cause and location tables, using the **numan-rtrv** MML command. Refer to the *Cisco Media Gateway Controller Software Release 7 Dial Plan Guide* for more information.
- If the result table does not contain all of the references, modify its value using the **numan-ed** MML command and reload the dial plan file using the **chg-dpl** MML command. Refer to the *Cisco Media Gateway Controller Software Release 7 Dial Plan Guide* for more information. Otherwise, proceed to Step 2.
- Step 2** Verify that the dial plan file was loaded correctly, using the procedure described in “Verifying Proper Loading of a Dial Plan” section on page 8-69.
-

ANAL:Cause_InvldRsIts_CauseTbl

This alarm occurs when cause analysis successfully reads the cause table but the value returned is logically invalid. Cause analysis gets two values from the cause table: an immediate result index and a location index. The immediate result index indicates that analysis should start reading results now, but the location index indicates that another table read is required to find the correct result table index. These results are logically incompatible. Most likely this results from a failure of the underlying software or a corruption of the cause table.

Corrective Action

To correct the problem identified by this alarm, verify that the dial plan file was loaded correctly, using the procedure described in “Verifying Proper Loading of a Dial Plan” section on page 8-69.

ANAL: Cause_MdfyBFail_AnnounceID

This alarm occurs during cause analysis when an announcement result is encountered and analysis is unable to replace the last 4 digits of the B-number with the announcement ID. This is commonly caused by an out-of-range announcement ID (it should be 0 to 9999) or a B-number less than 4 digits long.

Corrective Action

To correct the problem identified by this alarm, perform the following steps:

-
- | | |
|---------------|--|
| Step 1 | Verify that the affected announcement ID is within the range 0 through 9999, using the numan-rtrv MML command. Refer to the <i>Cisco Media Gateway Controller Software Release 7 Dial Plan Guide</i> for more information.

If the announcement ID is outside of the range, modify its value using the numan-ed MML command and proceed to Step 2. Refer to the <i>Cisco Media Gateway Controller Software Release 7 Dial Plan Guide</i> for more information. Otherwise, proceed to Step 2. |
| Step 2 | Verify that the affected B-number is at least 4 digits long, using the numan-rtrv MML command. Refer to the <i>Cisco Media Gateway Controller Software Release 7 Dial Plan Guide</i> for more information.

If the affected B-number is less than 4 digits long, modify its value using the numan-ed MML command. Refer to the <i>Cisco Media Gateway Controller Software Release 7 Dial Plan Guide</i> for more information. Otherwise, proceed to Step 3. |
| Step 3 | If you modified your dial plan, reload your dial plan file using the chg-dpl MML command. Otherwise, proceed to Step 4. |
| Step 4 | Verify that the dial plan file was loaded correctly, using the procedure described in “Verifying Proper Loading of a Dial Plan” section on page 8-69. |
-

ANAL: Cause_MdfyBFail_AppPtInvld

This alarm occurs during cause analysis when a B-number modification result is encountered and the application point (where digits are inserted) specified is beyond the end of the digit string. This is caused by an incorrect application point being specified in the result data, a corrupt result table, or incorrectly constructed cause analysis values.

Corrective Action

To correct the problem identified by this alarm, perform the following steps:

-
- Step 1** Verify that the specified application points in the result data is correct, using the **numan-rtrv** MML command. Refer to the *Cisco Media Gateway Controller Software Release 7 Dial Plan Guide* for more information.
- If any of the application points are incorrect, modify their value using the **numan-ed** MML command and reload the dial plan file using the **chg-dpl** MML command. Refer to the *Cisco Media Gateway Controller Software Release 7 Dial Plan Guide* for more information. Otherwise, proceed to Step 2.
- Step 2** Verify that the dial plan file was loaded correctly, using the procedure described in “Verifying Proper Loading of a Dial Plan” section on page 8-69.
-

ANAL: Cause_Rte_LoopDetected

This alarm occurs during cause analysis when a route or announcement result is encountered. In these cases, the indicated route identifier is checked against a list of previously provided results. If a match is found, this alarm is raised and an error is returned to call processing. This is done to prevent calls from endlessly routing to a single route or series of routes infinitely due to cause analysis interactions.

Corrective Action

To correct the problem identified by this alarm, verify that the dial plan file was loaded correctly, using the procedure described in “Verifying Proper Loading of a Dial Plan” section on page 8-69.

ANAL: CustId/StartIdx Missing

This alarm occurs when the property CustGrpId or BOrigStartIndex are not present on the associated SS7 signaling service or trunk group. These are required to find the correct place to begin analysis.

Corrective Action

To correct the problem identified by this alarm, perform the following steps:

-
- Step 1** Verify that the values of CustGrpId and BOrigStartIndex properties for the associated SS7 signaling service or trunk group are correct by logging in to the active Cisco MGC, starting an MML session, and entering the following command:

```
prov-rtrv:component:name="comp_name"
```

Where:

- *component*—MML component type name for the SS7 signaling service or trunk group properties. Enter one of the following:
 - sigsvccprop—Component type for SS7 signaling service properties.
 - trnkgrpprop—Component type for trunk group properties.
- *comp_name*—MML name for the affected SS7 signaling service or trunk group.

For example, if you wanted to verify the properties for an SS7 signaling service called **ss7svc1**, you would enter the following command:

```
prov-rtrv:sigsvccprop:name="ss7svc1"
```

If your system has been properly configured for dial plan use, the system returns a response similar to the following:

```
MGC-01 - Media Gateway Controller 2001-06-01 10:09:47
M   RTRV
    "session=active:sigsvccprop"
    /*
adjDestinations = 16
AlarmCarrier = 0
BOrigStartIndex = 0
BothwayWorking = 1
BTermStartIndex = 1
CctGrpCarrier = 2
CGBA2 = 0
CircHopCount = 0
CLIPess = 0
CotInTone = 2010
CotOutTone = 2010
CotPercentage = 0
CustGrpId=2222
dialogRange = 0
ExtCOT = Loop
ForwardCLiInIAM = 1
ForwardSegmentedNEED = 1
GLARE = 0
GRA2 = 0
GRSEnabled = false
InternationalPrefix = 0
layerRetries = 2
layerTimer = 10
MaxACL = 3
maxMessageLength = 250
mtp3Queue = 1024
NationalPrefix = 0
NatureOfAddrHandling = 0
Normalization = 0
OMaxDigits = 24
OMinDigits = 0
OOverlap = 0
OwnClIi = na
RedirMax = 3
ReleaseMode = Async
restartTimer = 10
RoutePref = 0
sendAfterRestart = 16
slsTimer = 300
srtTimer = 300
sstTimer = 300
standard = ANSI92
SwitchID = 0
TMaxDigits = 24
TMinDigits = 0
TOverlap = 0
variant = SS7-ANSI
VOIPPrefix = 0
```

- Step 2** If you need to modify your settings, start a provisioning session as described in the “Starting a Provisioning Session” section on page 3-63.

Step 3 If the BOrigStartIndex property is not set to 1, enter the following command:

```
prov-ed: component:name="comp_name",BOrigStartIndex=1
```

Where:

- *component*—MML component type name for the SS7 signaling service or trunk group properties. Enter one of the following:
 - *ss7path*—Component type for SS7 signaling services.
 - *trnkgp*—Component type for trunk groups.
- *comp_name*—MML name for the affected SS7 signaling service or trunk group.

Step 4 If the CustGrpId property is missing from the affected SS7 signaling service or trunk group, enter the following command:



Note If you are modifying the CustGrpId value for an SS7 signaling service, you must set that SS7 signaling service to the out-of-service administrative state, as described in the “Setting the Administrative State” section on page 8-70. Once you have entered the CustGrpId value, you can return the SS7 signaling service to the in-service administrative state. You do not have to change the administrative state when you are

```
prov-ed: component:name="comp_name",CustGrpId=number
```

Where:

- *component*—MML component type name for the SS7 signaling service or trunk group properties. Enter one of the following:
 - *ss7path*—Component type for SS7 signaling services.
 - *trnkgp*—Component type for trunk groups.
- *comp_name*—MML name for the SS7 signaling service or trunk group on which you are mapping the internal maximum ACL value to the value expected by the adjacent signaling point.
- *number*—Customer group ID number that is associated with your dial plan.

Step 5 Save and activate your provisioning session as described in the “Saving and Activating your Provisioning Changes” section on page 3-64.

ANAL: Data Failure Rcvd

This alarm occurs when during analysis, a data failure is found in the external routing engine.

Corrective Action

To correct the problem identified by this alarm, verify that the dial plan file was loaded correctly, using the procedure described in “Verifying Proper Loading of a Dial Plan” section on page 8-69.

ANAL: InvalidtrkGrpType

This alarm occurs when the analysis module has not provided a valid trunk group type. The problem occurs if the route analysis table specifies an invalid trunk group type.

Corrective Action

To correct the problem identified by this alarm, perform the following steps:

-
- Step 1** Display the valid trunk group types using the **prov-rtrv** MML command as described in the “Retrieving Provisioning Data” section on page 3-67.
 - Step 2** Correct the invalid trunk group type in the route analysis table using the **numan-ed** MML command and reload the dial plan using the **chg-dpl** MML command. Refer to the *Cisco Media Gateway Controller Software Release 7 Dial Plan Guide* for more information.
-

ANAL: Prof_GetFail_DigModTbl

This alarm occurs during profile analysis when a B-number modification result is encountered and the digit modification string is unreadable. This can be due to the digit modification table being corrupted or an incorrect digit modification index being stored in the B-number modification result's data.

Corrective Action

To correct the problem identified by this alarm, verify that the dial plan file was loaded correctly, using the procedure described in “Verifying Proper Loading of a Dial Plan” section on page 8-69.

ANAL: Prof_GetFail_InvldRslt

This alarm occurs during profile analysis when a result is encountered that is not supported in profile analysis. This is due to corruption of either the NOA or NPI tables or the result table.

Corrective Action

To correct the problem identified by this alarm, verify that the dial plan file was loaded correctly, using the procedure described in “Verifying Proper Loading of a Dial Plan” section on page 8-69.

ANAL: Prof_GetFail_NOATbl

This alarm occurs during profile analysis when the NOA table is unreadable. This can be due to the NOA table being corrupted, a failure in the underlying software, or the NOA table being built without all the existing call context NOA values.

Corrective Action

To correct the problem identified by this alarm, perform the following steps:

-
- Step 1** Verify that the NOA table uses all of the existing call context NOA values using the **numan-rtrv** MML command. Refer to the *Cisco Media Gateway Controller Software Release 7 Dial Plan Guide* for more information.

If the NOA table is missing any of the existing call context NOA values, add them using the **numan-ed** MML command and reload the dial plan file using the **chg-dpl** MML command. Refer to the *Cisco Media Gateway Controller Software Release 7 Dial Plan Guide* for more information. Otherwise, proceed to Step 2.

- Step 2** Verify that the dial plan file was loaded correctly, using the procedure described in “Verifying Proper Loading of a Dial Plan” section on page 8-69.
-

ANAL: Prof_GetFail_NPITbl

This alarm occurs during profile analysis when the NPI table is unreadable. This can be due to the NPI table being corrupted, a failure in the underlying software, or the NPI table not being fully populated with all the possible references from the NOA table.

Corrective Action

To correct the problem identified by this alarm, perform the following steps:

-
- Step 1** Verify that the NPI table uses all of the possible references from the NOA table using the **numan-rtrv** MML command. Refer to the *Cisco Media Gateway Controller Software Release 7 Dial Plan Guide* for more information.
- If the NPI table is missing any of the references from the NOA table, add them using the **numan-ed** MML command and reload the dial plan file using the **chg-dpl** MML command. Refer to the *Cisco Media Gateway Controller Software Release 7 Dial Plan Guide* for more information. Otherwise, proceed to Step 2.
- Step 2** Verify that the dial plan file was loaded correctly, using the procedure described in “Verifying Proper Loading of a Dial Plan” section on page 8-69.
-

ANAL: Prof_GetFail_RsltTbl

This alarm occurs during profile analysis when the result table is unreadable. This can be due to the result table being corrupted, a failure in the underlying software, or the result table not being fully populated with all the possible references from the NOA or NPI tables.

Corrective Action

To correct the problem identified by this alarm, perform the following steps:

-
- Step 1** Verify that the result table uses all of the possible references from the NOA and NPI tables using the **numan-rtrv** MML command. Refer to the *Cisco Media Gateway Controller Software Release 7 Dial Plan Guide* for more information.
- If the result table is missing any of the references from the NOA and NPI tables, add them using the **numan-ed** MML command and reload the dial plan file using the **chg-dpl** MML command. Refer to the *Cisco Media Gateway Controller Software Release 7 Dial Plan Guide* for more information. Otherwise, proceed to Step 2.
- Step 2** Verify that the dial plan file was loaded correctly, using the procedure described in “Verifying Proper Loading of a Dial Plan” section on page 8-69.
-

ANAL: Prof_InvldNPAValue

This alarm occurs during profile analysis when a 7-digit B-number is encountered and the NPA property is set against the originating trunk group. An NPA string of more or less than 3 characters is invalid. This is most likely caused by data corruption.

Corrective Action

To correct the problem identified by this alarm, perform the following steps:

-
- | | |
|---------------|--|
| Step 1 | Verify that the NPA values have been properly provisioned for the trunk group using the numan-rtrv MML command. Refer to the <i>Cisco Media Gateway Controller Software Release 7 Dial Plan Guide</i> for more information.

If the NPA values are incorrect, modify them using the numan-ed MML command and reload the dial plan file using the chg-dpl MML command. Refer to the <i>Cisco Media Gateway Controller Software Release 7 Dial Plan Guide</i> for more information. Otherwise, proceed to Step 2. |
| Step 2 | Verify that the dial plan file was loaded correctly, using the procedure described in “Verifying Proper Loading of a Dial Plan” section on page 8-69. |
-

ANAL: Prof_InvRsIts_NOATbl

This alarm occurs when profile analysis successfully reads the NOA table but the value returned is logically invalid. Profile analysis gets two values from the NOA table: an immediate result index and an NPI index. An immediate result index indicates that analysis should start reading results now but an NPI index indicates that another table read is required to find the correct result table index. These results are logically incompatible. Most likely this results from a failure of the underlying software or a corruption of the NOA table.

Corrective Action

To correct the problem identified by this alarm, verify that the dial plan file was loaded correctly, using the procedure described in “Verifying Proper Loading of a Dial Plan” section on page 8-69.

ANAL: Prof_MdfyBFail_AppPtInvld

This alarm occurs during profile analysis when a B-number modification result is encountered and the specified application point (where digits are inserted) is beyond the end of the digit string. This is caused by an incorrect application point being specified in the result data, a corrupt result table, or incorrectly constructed Profile analysis values.

Corrective Action

To correct the problem identified by this alarm, perform the following steps:

-
- | | |
|---------------|--|
| Step 1 | Verify that the specified application points in the result data is correct, using the numan-rtrv MML command. Refer to the <i>Cisco Media Gateway Controller Software Release 7 Dial Plan Guide</i> for more information. |
|---------------|--|
-

If any of the application points are incorrect, modify their value using the **numan-ed** MML command and reload the dial plan file using the **chg-dpl** MML command. Refer to the *Cisco Media Gateway Controller Software Release 7 Dial Plan Guide* for more information. Otherwise, proceed to Step 2.

- Step 2** Verify that the dial plan file was loaded correctly, using the procedure described in “Verifying Proper Loading of a Dial Plan” section on page 8-69.
-

ANAL: RteStartIndexInvalid

This alarm occurs when the start index for the route analysis table is invalid.

Corrective Action

To correct the problem identified by this alarm, perform the following steps:

-
- Step 1** Verify that the data for the provisioned route lists is correct by logging in to the active Cisco MGC, starting an MML session, and entering the following command:
- ```
prov-rtrv:rtlist:"all"
```
- Step 2** If there is incorrect data for the route lists, correct it by using the **prov-ed** MML command. Otherwise, proceed to Step 3. Refer to the *Cisco Media Gateway Controller Software Release 7 Provisioning Guide* for more information on provisioning route lists.
- Step 3** Contact the Cisco TAC to further analyze the problem and determine a solution. For more information about contacting the Cisco TAC, refer to the “Obtaining Technical Assistance” section on page xviii.
- 

## ANAL: RteTableFail\_GetRteList

This alarm occurs when access to the route list failed. The problem occurs if the index to the route list is not valid or if the route list is not loaded.

### Corrective Action

To correct the problem identified by this alarm, verify that the dial plan file was loaded correctly, using the procedure described in “Verifying Proper Loading of a Dial Plan” section on page 8-69.

## ANAL: RteTableFail\_GetTrkAttrdata

This alarm occurs when access to the trunk group attribute data table failed. The problem occurs if the index to the trunk group attribute data table is not valid or if the table is not loaded.

### Corrective Action

To correct the problem identified by this alarm, verify that the dial plan file was loaded correctly, using the procedure described in “Verifying Proper Loading of a Dial Plan” section on page 8-69.

## ANAL: RteTableFail\_GetTrkGrpdata

This alarm occurs when access to the trunk group data failed. The problem occurs if the index to the trunk group data is not valid or if the trunk group data table is not loaded.

### Corrective Action

To correct the problem identified by this alarm, verify that the dial plan file was loaded correctly, using the procedure described in “Verifying Proper Loading of a Dial Plan” section on page 8-69.

## ANAL: RteTableFail\_GetTrunkList

This alarm occurs when access to the trunk group list failed. The problem occurs if the index to the trunk group list is not valid or if the trunk group list is not loaded.

### Corrective Action

To correct the problem identified by this alarm, verify that the dial plan file was loaded correctly, using the procedure described in “Verifying Proper Loading of a Dial Plan” section on page 8-69.

## ANAL: TrunkGrpRsItCtrExceeded

This alarm occurs when the analysis module has provided the maximum number of candidate trunk groups allowed. The maximum number is 20. The purpose of the alarm is to limit the time spent searching for candidate trunk groups.

### Corrective Action

To correct the problem identified by this alarm, verify that the dial plan file was loaded correctly, using the procedure described in “Verifying Proper Loading of a Dial Plan” section on page 8-69.

## C7LNK ALGNMT LOST

This alarm occurs when the MTP2 for the C7 link between a Cisco SLT and an associated APC has lost alignment.

### Corrective Action

To correct the problem identified by this alarm, use the diagnostics on the affected Cisco SLT to determine why the link has lost alignment, as described in the “Verifying the Link Alignment Status” section on page B-6.

## C7DPC CONGESTION

This alarm occurs when a link in a signaling route towards a given DPC becomes congested or when a DPC is congested and has sent a congestion indication to the Cisco MGC.

## Corrective Action

To correct the problem identified by this alarm, perform the following steps:

- 
- |               |                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|---------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | Verify the status of the links associated with the affected DPC, as described in the “Retrieving the Service State of a Linkset” section on page 3-51.<br><br>If none of the links are out-of-service, this alarm has occurred because the DPC is congested. In this instance, corrective action is not necessary, and you must wait for the congestion condition to clear.<br><br>If any of the links are out-of-service, proceed to Step 2. |
| <b>Step 2</b> | Return the out-of-service links to service, as described in the “Setting the Service State of a Link or Linkset” section on page 8-60.<br><br>If that does not resolve the problem, proceed to Step 3.                                                                                                                                                                                                                                        |
| <b>Step 3</b> | Contact the Cisco TAC to further analyze the problem and determine a solution. For more information about contacting the Cisco TAC, refer to the “Obtaining Technical Assistance” section on page xviii.                                                                                                                                                                                                                                      |
- 

## C7LNK CONGESTION

This alarm occurs when that the SS7 MTP2 link has encountered congestion such that it cannot receive any more messages. This alarm applies only to SS7 links that are terminated on I/O cards.

## Corrective Action

To correct the problem identified by this alarm, perform the following steps:

- 
- |               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|---------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | Reengineer your call traffic to reduce the number of calls coming to the affected link. If that resolves the problem, the procedure is complete. Otherwise, proceed to Step 2.                                                                                                                                                                                                                                                                                                                                   |
| <b>Step 2</b> | Add more links to the linkset associated with the affected link. To do this, you must either add additional I/O cards, or switch to Cisco SLTs. For more information on installing the I/O cards or Cisco SLTs, refer to the <i>Cisco Media Gateway Controller Hardware Installation Guide</i> . For more information on provisioning your new links, refer to the <i>Cisco Media Gateway Controller Software Release 7 Provisioning Guide</i> .<br><br>If that does not resolve the problem, proceed to Step 3. |
| <b>Step 3</b> | Contact the Cisco TAC to further analyze the problem and determine a solution. For more information about contacting the Cisco TAC, refer to the “Obtaining Technical Assistance” section on page xviii.                                                                                                                                                                                                                                                                                                         |
- 

## C7LNK INHIBIT

This alarm occurs when a C7 link has been inhibited for maintenance.

## Corrective Action

To correct the problem identified by this alarm, uninhibit the specified C7 link, as described in the “Setting the Service State of a Link or Linkset” section on page 8-60, when the maintenance is complete.

## Config Fail

This alarm occurs when the configuration has failed.

### Corrective Action

To correct the problem identified by this alarm, perform the following steps:

- 
- Step 1** Search the active system log file, as described in the “Viewing System Logs” section on page 8-4, for logs that indicate errors in the content of your provisioning data.
- If there are no logs that indicate errors in the content of your provisioning data, proceed to Step 2.
- If there are logs that indicate errors in the content of your provisioning data, start a dynamic reconfiguration session to change the settings for the component(s) identified in the log message(s), as described in the “Invoking Dynamic Reconfiguration” section on page 3-65.
- If that corrects the problem, the procedure is complete. Otherwise, proceed to Step 2.
- Step 2** Contact the Cisco TAC to further analyze the problem and determine a solution. For more information about contacting the Cisco TAC, refer to the “Obtaining Technical Assistance” section on page xviii.
- 

## DISK

This alarm occurs when the system disk is running out of space.

### Corrective Action

To correct the problem identified by this alarm, delete any unnecessary files from your Cisco MGC, as described in the “Deleting Unnecessary Files to Increase Available Disk Space” section on page 8-112.

## Ext Node Interface Fail

This alarm is generated when an SRCP session loses heartbeats with the remote gateway, indicating that the link to the gateway is down.

### Corrective Action

To correct the problem identified by this alarm, perform the following steps:

- 
- Step 1** Verify that the remote media gateway is up and running by checking its LEDs. Refer to the documentation associated with the remote media gateway for more information on verifying its functioning using the LEDs.
- If the remote gateway is not up and working, restore it to service using the procedures found in the documentation associated with the remote media gateway.
- If the remote gateway is up and running, proceed to Step 2.
- Step 2** Verify that the Ethernet interfaces between the Cisco MGC and the associated media gateway are working properly.



**Note**

Information on verifying the proper operation of an Ethernet interface on the Cisco MGC host can be found in the Sun Microsystems documentation that came with your system. Information on verifying the proper functioning of an Ethernet interface on the media gateway can be found in its associated documentation.

If an element of the Ethernet connection (such as a cable or an Ethernet interface card) is not working properly, replace it. Otherwise, proceed to Step 3.

**Note**

Information on removing and replacing an Ethernet interface card on the Cisco MGC host can be found in the Sun Microsystems documentation that came with your system. Information on removing and replacing an Ethernet interface card on the media gateway can be found in its associated documentation.

**Step 3** Verify that the near-end and far-end SRCP sessions are operating normally.

**Step 4** If that does not resolve the problem, contact the Cisco TAC to further analyze the problem and determine a solution. For more information about contacting the Cisco TAC, refer to the .

## FAIL

This alarm occurs when the component referenced in the alarm has failed. The failure may be service affecting, in which case other alarms are raised.

### Corrective Action

To correct the problem identified by this alarm, perform the following steps:

**Step 1** If the component identified in the alarm text is in the system software, contact the Cisco TAC to further analyze the problem and determine a solution. For more information about contacting the Cisco TAC, refer to the .

If the component identified in the alarm text is a piece of system hardware, you should restart the component's software. Procedures for stopping and restarting the software of any of the elements of the Cisco MGC node can be found in Chapter 2, "Cisco MGC Node Component Startup and Shutdown Procedures". If that does not resolve the problem, proceed to Step 2.

**Step 2** Replace the component identified in the alarm text. Procedures for replacing Cisco MGC host hardware can be found in the associated Sun Microsystems documentation. Procedures for replacing Cisco SLT hardware can be found in "Replacing a Cisco SLT" section on page 6-6. Procedures for replacing Cisco Catalyst 5500 MSR hardware can be found in "Replacing Hardware Components" section on page 7-5.

**Step 3** Contact the Cisco TAC to further analyze the problem and determine a solution. For more information about contacting the Cisco TAC, refer to the .

## FailoverPeerLost

This alarm occurs when the failover daemon on the standby Cisco MGC is not reachable.

## Corrective Action

To correct the problem identified by this alarm, perform the following steps:

- Step 1** Verify that the Ethernet interfaces between the active and standby Cisco MGCs and the Cisco Catalyst 5500 MSRs are working properly.



**Note** Information on verifying the proper operation of an Ethernet interface on the Cisco MGC host can be found in the Sun Microsystems documentation that came with your system. Information on verifying the proper functioning of an Ethernet interface on the Cisco Catalyst 5500 MSRs can be found in the “Checking Equipment Status” section on page 7-1.

If an element of the Ethernet connection (such as a cable or an Ethernet interface card) is not working properly, replace it. Otherwise, proceed to Step 2.



**Note** Information on removing and replacing an Ethernet interface card on the Cisco MGC host can be found in the Sun Microsystems documentation that came with your system. Information on removing and replacing an Ethernet interface card on the Cisco Catalyst 5500 MSRs can be found in the “Replacing Hardware Components” section on page 7-5.

- Step 2** Contact the Cisco TAC to further analyze the problem and determine a solution. For more information about contacting the Cisco TAC, refer to the “Obtaining Technical Assistance” section on page xviii.

## FailoverPeer00S

This alarm occurs when the failover daemon goes out-of-service in the standby Cisco MGC.

## Corrective Action

To correct the problem identified by this alarm, check the alarms on the standby Cisco MGC, using the procedure in the “Retrieving All Active Alarms” section on page 8-3, and resolve those alarms.

## Gen Fail

This alarm occurs when a failure has occurred due to resource exhaustion or configuration problems, including:

- Memory exhaustion.
- Queue overflow.
- Message congestion.
- IPC file cannot be opened.
- A timer has expired.

Log messages in the active system log file indicate the nature of the failure. For the majority of the failures, this alarm is informational and no user action is required. When this alarm is generated because an IPC file cannot be opened, you must take corrective action.

## Corrective Action

To correct the problem identified by this alarm, perform the following steps:

- 
- Step 1** Search the active system log file, as described in the “Viewing System Logs” section on page 8-4, for logs that indicate that an IPC file cannot be opened.
- If there are no logs that indicate that an IPC file cannot be opened, no further action is required.
- If there are logs that indicate that an IPC file cannot be opened, proceed to Step 2.
- Step 2** Shut down the Cisco MGC software on your standby Cisco MGC, as described in the “Shutting Down the Cisco MGC Software Manually” section on page 2-4.
- Step 3** Restart the Cisco MGC software on your standby Cisco MGC, as described in the “Starting the Cisco MGC Software” section on page 2-2.
- Step 4** Perform a manual switchover, as described in the “Performing a Manual Switchover” section on page 3-80.
- Step 5** Shut down the Cisco MGC software on your newly standby Cisco MGC, as described in the “Shutting Down the Cisco MGC Software Manually” section on page 2-4.
- Step 6** Restart the Cisco MGC software on your newly standby Cisco MGC, as described in the “Starting the Cisco MGC Software” section on page 2-2.
- If that resolves the problem, the procedure is complete. Otherwise, proceed to Step 7.
- Step 7** Contact the Cisco TAC to further analyze the problem and determine a solution. For more information about contacting the Cisco TAC, refer to the “Obtaining Technical Assistance” section on page xviii.
- 

## IP CONNECTION FAILED

This alarm occurs when the Cisco MGC loses network (IP) connectivity to a Cisco SLT. This alarm is generated for each SS7 link associated with the affected Cisco SLT.

## Corrective Action

To correct the problem identified by this alarm, perform the following steps:

- 
- Step 1** Verify that the affected Cisco SLT is up and running by performing the procedures in the “Checking Equipment Status” section on page 6-2.
- If the affected Cisco SLT is not up and running, start it using the procedure in the “Cisco Signaling Link Terminal Startup Procedure” section on page 2-3. If this does not resolve the problem, replace the affected Cisco SLT as described in the “Replacing a Cisco SLT” section on page 6-6.
- If the affected Cisco SLT is up and running, proceed to Step 2.
- Step 2** Verify that the Ethernet interfaces between the Cisco MGC and the affected Cisco SLT are working properly.



**Note** Information on verifying the proper operation of an Ethernet interface on the Cisco MGC host can be found in the Sun Microsystems documentation that came with your system. Information on verifying the proper functioning of an Ethernet interface on the Cisco SLT can be found in the “Checking Equipment Status” section on page 6-2.

---

If an element of the Ethernet connection (such as a cable or an Ethernet interface card) is not working properly, replace it. Otherwise, proceed to Step 3.



**Note** Information on removing and replacing an Ethernet interface card on the Cisco MGC host can be found in the Sun Microsystems documentation that came with your system. Information on removing and replacing components on the Cisco SLT can be found in the “Replacing Hardware Components” section on page 6-13.

- Step 3** Contact the Cisco TAC to further analyze the problem and determine a solution. For more information about contacting the Cisco TAC, refer to the “Obtaining Technical Assistance” section on page xviii.

## IP RTE CONF FAIL

This alarm occurs when a signaling channel is not using the route that it is was configured to use.

### Corrective Action

To correct the problem identified by this alarm, perform the following steps:

- Step 1** Verify that the provisioned settings for the identified IP route are correct, using the **prov-rtrv** MML command, as described in the “Retrieving Provisioning Data” section on page 3-67.
- If the provisioned settings for your IP route are correct, proceed to Step 2.
- If the provisioned settings for your IP route are incorrect, start a dynamic reconfiguration session to change the settings, as described in the “Invoking Dynamic Reconfiguration” section on page 3-65.
- Step 2** Contact the Cisco TAC to further analyze the problem and determine a solution. For more information about contacting the Cisco TAC, refer to the “Obtaining Technical Assistance” section on page xviii.

## IP RTE FAIL

This alarm occurs when a signaling channel that is provisioned with a next hop address if the system failed to add the required route.

### Corrective Action

To correct the problem identified by this alarm, perform the following steps:

- Step 1** Verify that the provisioned settings for the identified IP route are correct, using the **prov-rtrv** MML command, as described in the “Retrieving Provisioning Data” section on page 3-67.
- If the provisioned settings for your IP route are correct, proceed to Step 2.
- If the provisioned settings for your IP route are incorrect, start a dynamic reconfiguration session to change the settings, as described in the “Invoking Dynamic Reconfiguration” section on page 3-65.

- Step 2** Contact the Cisco TAC to further analyze the problem and determine a solution. For more information about contacting the Cisco TAC, refer to the “Obtaining Technical Assistance” section on page xviii.
- 

## ISUP: COT Failure

This alarm occurs when a COT message was received indicating a failed continuity test.

### Corrective Action

To correct the problem identified by this alarm, run a manual COT test, as described in the “Running a Manual Continuity Test” section on page 8-96.

## LIF BER

This alarm occurs when an excessive bit error ratio is detected from a frame alignment signal. This might be caused by any source of electrical noise; for example, degraded transmission line, degraded line connectors, high-voltage electrical source located in proximity of line.

### Corrective Action

To correct the problem identified by this alarm, isolate the source by testing the connections and transmission line for the identified component. When you have identified the source, resolve as necessary.

## LIF FAIL

This alarm occurs when line interface (LIF) has failed. All physical lines to the Cisco MGC can raise this alarm.

### Corrective Action

To correct the problem identified by this alarm, perform the following steps:

- 
- Step 1** Verify that the provisioned settings for the identified line interface are correct, using the **prov-rtrv** MML command, as described in the “Retrieving Provisioning Data” section on page 3-67.
- If the provisioned settings for your line interface are correct, proceed to Step 4.
- If the provisioned settings for your line interface are incorrect, proceed to Step 2.
- Step 2** Place the identified line interface in the out-of-service administrative state, as described in the “Setting the Administrative State” section on page 8-70.
- Start a dynamic reconfiguration session to change the settings, as described in the “Invoking Dynamic Reconfiguration” section on page 3-65.
- Step 3** Place the identified line interface in the in-service administrative state, as described in the “Setting the Administrative State” section on page 8-70.
- If that does not resolve the problem, proceed to Step 4.

- Step 4** Contact the Cisco TAC to further analyze the problem and determine a solution. For more information about contacting the Cisco TAC, refer to the “Obtaining Technical Assistance” section on page xviii.
- 

## LIF LOF

This alarm occurs when a loss of T1/E1 framing has been detected on the LIF. The physical line has a signal but has lost the framing pattern.

### Corrective Action

To correct the problem identified by this alarm, perform the following steps:

- 
- Step 1** Verify that the framing format used on the port matches the framing format used on the line.  
If the framing formats are different, change the framing format on the port to the other framing format. Otherwise, proceed to Step 2. If the alarm does not clear, proceed to Step 2.
- Step 2** Change the line build-out setting. If the alarm does not clear, proceed to Step 3.
- Step 3** Open the statistics report for the port and look for evidence of a bad line. Bursts of Latvia could indicate a timing problem.  
If you find evidence of a bad line, perform loopback tests on the line to isolate the problem. Otherwise, proceed to Step 4. Once you have isolated the problem, resolve as necessary. If the alarm does not clear, proceed to Step 4.
- Step 4** Contact the Cisco TAC to further analyze the problem and determine a solution. For more information about contacting the Cisco TAC, refer to the “Obtaining Technical Assistance” section on page xviii.
- 

## LIF LOS

This alarm occurs when the transmitted signal is lost in the T1/E1. The receiving end does not receive the signal. The physical line might have a break in it.

### Corrective Action

To correct the problem identified by this alarm, perform the following steps:

- 
- Step 1** Verify that the cable connections are correct between the interface port and your service provider’s equipment or T1/E1 terminal equipment.  
If the cable was built on-site, check the cable connectors. A reversal of transmit and receive pairs or an open receive pair can cause this condition.  
If the cable connections appear correct, then proceed to Step 2.
- Step 2** Check your T1/E1 equipment, or ask your service provider to test your T1/E1 line and correct any errors found.  
If the alarm does not clear, then proceed to Step 2.

- Step 3** Contact the Cisco TAC to further analyze the problem and determine a solution. For more information about contacting the Cisco TAC, refer to the “Obtaining Technical Assistance” section on page xviii.
- 

## LIF SES

This alarm occurs when the LIF is automatically set to the out-of-service state because of severely errored seconds. The TDM line has a large amount of noise, causing an error rate greater than 10<sup>-3</sup>. Framing and signal are within tolerance. This indicates a degraded but functioning line.

### Corrective Action

To correct the problem identified by this alarm, perform the following steps:

- 
- Step 1** Verify that the terminations and cabling for the LIF are working. If you can identify the source of the problem, resolve as necessary. Otherwise, proceed to Step 2.
- Step 2** Contact the Cisco TAC to further analyze the problem and determine a solution. For more information about contacting the Cisco TAC, refer to the “Obtaining Technical Assistance” section on page xviii.
- 

## LIF YELLOW

This alarm occurs when the receiving end is reporting a loss of the transmitted signal. This is reported for T1/E1 facilities only.

### Corrective Action

To correct the problem identified by this alarm, perform the following steps:

- 
- Step 1** Connect an external loopback cable to the affected port.
- If no alarms are produced, proceed to Step 2
- If alarms are produced, the port is causing the error. Replace the hardware component associated with the port. Refer to the associated media gateway documentation for more information on replacing the component.
- Step 2** Check for an open, short, or wiring error in the cable between the network interface port and your service provider’s network interface unit T1/E1 terminal equipment. An open transmit pair can cause this condition.
- If you find a wiring problem, replace the cable. If that does not clear the alarm, proceed to Step 3.
- If you do not find a wiring problem, then proceed to Step 3.
- Step 3** If your port is configured to use D4 framing, the port may intermittently detect yellow alarms because the packet data may contain the pattern that is used to signal yellow alarm in D4 framing. If it is possible, switch to ESF framing in both the terminal equipment and the line equipment.
- If that does not clear the alarm, proceed to Step 4.

- Step 4** Contact the Cisco TAC to further analyze the problem and determine a solution. For more information about contacting the Cisco TAC, refer to the “Obtaining Technical Assistance” section on page xviii.
- 

## LIF: IDLE CHANGE

This alarm occurs when the physical line has failed because its cable is broken or not plugged in. This is reported for V.35 facilities only.

### Corrective Action

To correct the problem identified by this alarm, perform the following steps:

- 
- Step 1** Verify that the V.35 cables between the port and the far-end are working correctly.
- If you find a problem with a V.35 cable, replace the cable. If that does not correct the problem, proceed to Step 2.
- If you do not find a problem with the V.35 cables, proceed to Step 2.
- Step 2** Contact the Cisco TAC to further analyze the problem and determine a solution. For more information about contacting the Cisco TAC, refer to the “Obtaining Technical Assistance” section on page xviii.
- 

## LIF: LOST CD

This alarm occurs when the physical line has failed because its cable is broken or not plugged in. This is reported for V.35 facilities only.

### Corrective Action

To correct the problem identified by this alarm, perform the following steps:

- 
- Step 1** Verify that the V.35 cables between the port and the far-end are working correctly.
- If you find a problem with a V.35 cable, replace the cable. If that does not correct the problem, proceed to Step 2.
- If you do not find a problem with the V.35 cables, proceed to Step 2.
- Step 2** Contact the Cisco TAC to further analyze the problem and determine a solution. For more information about contacting the Cisco TAC, refer to the “Obtaining Technical Assistance” section on page xviii.
- 

## LIF: LOST CTS

This alarm occurs when the physical line has failed because its cable is broken or not plugged in. This is reported for V.35 facilities only.



### Corrective Action

To correct the problem identified by this alarm, perform the following steps:

- 
- Step 1** Verify that the V.35 cables between the port and the far-end are working correctly.
- If you find a problem with a V.35 cable, replace the cable. If that does not correct the problem, proceed to Step 2.
- If you do not find a problem with the V.35 cables, proceed to Step 2.
- Step 2** Contact the Cisco TAC to further analyze the problem and determine a solution. For more information about contacting the Cisco TAC, refer to the “Obtaining Technical Assistance” section on page xviii.
- 

### MMDB: Database unavailable

This alarm occurs when the main memory database is currently unavailable to provide any services. Recovery is attempted and the alarm clears when or if the database becomes available.

### Corrective Action

To correct the problem identified by this alarm, delete any unnecessary files from your Cisco MGC, as described in the “Deleting Unnecessary Files to Increase Available Disk Space” section on page 8-112.

### MMDB: Database cause failover

This alarm occurs when the main memory database is currently unavailable on a redundant system and is indicating that the system should failover. Recovery is attempted and the alarm clears when or if the database becomes available.

### Corrective Action

To correct the problem identified by this alarm, delete any unnecessary files from your standby Cisco MGC, as described in the “Deleting Unnecessary Files to Increase Available Disk Space” section on page 8-112.

### MMDB: Database nearly full

This alarm occurs when the main memory database has detected that allocated resources for data storage are nearly all utilized.

### Corrective Action

To correct the problem identified by this alarm, delete any unnecessary files from your Cisco MGC, as described in the “Deleting Unnecessary Files to Increase Available Disk Space” section on page 8-112.

### NAS: AuditResponse Failure

This alarm occurs when the identified media gateway fails to send a RESYNC RESP message back to the Cisco MGC within the audit time interval.

## Corrective Action

To correct the problem identified by this alarm, perform the following steps:

- 
- Step 1** Verify that the affected media gateway is in the in-service state, as described in the “Retrieving Signaling Channel Attributes” section on page 3-48 and the “Verifying the Status of all Destinations” section on page 3-8.
- If the affected media gateway is in-service, proceed to Step 2. Otherwise, proceed to Step 3.
- Step 2** Verify that the configuration of the affected media gateway is correct. Refer to the documentation for the media gateway for more information.
- If that does not resolve the problem, proceed to Step 4.
- Step 3** Verify that the Ethernet interfaces between the Cisco MGC and the associated media gateway are working properly.



**Note** Information on verifying the proper operation of an Ethernet interface on the Cisco MGC host can be found in the Sun Microsystems documentation that came with your system. Information on verifying the proper functioning of an Ethernet interface on the media gateway can be found in its associated documentation.

---

If an element of the Ethernet connection (such as a cable or an Ethernet interface card) is not working properly, replace it. Otherwise, proceed to Step 4.



**Note** Information on removing and replacing an Ethernet interface card on the Cisco MGC host can be found in the Sun Microsystems documentation that came with your system. Information on removing and replacing an Ethernet interface card on the media gateway can be found in its associated documentation.

---

- Step 4** Contact the Cisco TAC to further analyze the problem and determine a solution. For more information about contacting the Cisco TAC, refer to the “Obtaining Technical Assistance” section on page xviii.
- 

## NAS: CommsFailure

This alarm occurs when the Cisco MGC cannot communicate with the identified media gateway.

## Corrective Action

To correct the problem identified by this alarm, perform the following steps:

- 
- Step 1** Determine whether the affected media gateway is up and running. Refer to the documentation for the media gateway for more information.
- If the affected media gateway is not up and running, restore it to service. Refer to the documentation for the media gateway for more information.
- If the affected media gateway is up and running, proceed to Step 2.
- Step 2** Verify that the IP configuration parameters for the Cisco MGC and the affected media gateway are correct.

**Note**

Use the **prov-rtrv** MML command, as described in the “Retrieving Provisioning Data” section on page 3-67, to retrieve the IP configuration information for the Cisco MGC. Refer to the documentation for the media gateway for information on retrieving the IP configuration data.

If the configuration of your Cisco MGC is incorrect, begin a dynamic reconfiguration session, as described in the “Invoking Dynamic Reconfiguration” section on page 3-65.

If the configuration of the affected media gateway is incorrect, modify the provisioning data for your system. Refer to the documentation for the media gateway for more information.

If the configuration of both the Cisco MGC and the affected media gateway are correct, then proceed to Step 3.

- Step 3** Contact the Cisco TAC to further analyze the problem and determine a solution. For more information about contacting the Cisco TAC, refer to the “Obtaining Technical Assistance” section on page xviii.

## NAS: ResourceFailure

This alarm occurs when a continuity test (COT) has not been acknowledged by the indicated media gateway.

### Corrective Action

To correct the problem identified by this alarm, run a manual COT on the indicated media gateway, as described in the Running a Manual Continuity Test, page 8-96.

## OOS TRAFFIC RE-ROUTE

This alarm occurs when the traffic channels (bearer channels, IP network) on one side of the Cisco MGC have been lost, causing the Cisco MGC to reroute channels away from the affected component. This is generally due to a network or equipment failure, but might be due to a provisioning failure.

### Corrective Action

To correct the problem identified by this alarm, perform the following steps:

- Step 1** Other alarms associated with the affected component should also be displayed. Resolve those alarms first.
- If resolving those alarms does not clear this alarm, proceed to Step 2.
- Step 2** Verify that the traffic channel provisioning settings for the Cisco MGC and the affected media gateway are correct.

**Note**

Use the **prov-rtrv** MML command, as described in the “Retrieving Provisioning Data” section on page 3-67, to retrieve the traffic channel provisioning data for the Cisco MGC. Refer to the documentation for the media gateway for information on retrieving the traffic channel data.

If the configuration of your Cisco MGC is incorrect, begin a dynamic reconfiguration session, as described in the “Invoking Dynamic Reconfiguration” section on page 3-65.

If the configuration of the affected media gateway is incorrect, modify the provisioning data for your system. Refer to the documentation for the media gateway for more information.

If the configuration of both the Cisco MGC and the affected media gateway are correct, then proceed to Step 3.

- Step 3** Contact the Cisco TAC to further analyze the problem and determine a solution. For more information about contacting the Cisco TAC, refer to the “Obtaining Technical Assistance” section on page xviii.
- 

## OverloadHeavy

This alarm occurs when the system has reached the threshold for overload level 3. The system performs an automatic switchover operation. If the call rejection percentage setting for overload level 3 is unchanged from its default value, all new calls are rejected until the abate threshold for overload level 3 is reached. This alarm is automatically cleared at that time. For more information, refer to the “Managing Automatic Congestion Control” section on page 3-75.

### Corrective Action

If this alarm is caused by a rare spike in traffic, corrective action is not necessary. If this alarm occurs regularly, you should ensure that your links and routes are properly configured for load sharing, as described in the “SS7 Load Sharing Malfunction” section on page 8-52, and re-route some of your traffic to other Cisco MGCs.



#### Note

This alarm can occur when a provisioning session is active during peak busy hours. If this should happen, the alarm can be cleared by stopping the provisioning session. For more information on the MML commands to manage a provisioning session, refer to the “Provisioning your Cisco MGC” section on page 3-63.

---

## OverloadMedium

This alarm occurs when the system has reached the threshold for overload level 2. A percentage of new calls, based on the call rejection percentage setting for overload level 2, are rejected until the abate threshold for overload level 2 is reached. This alarm is automatically cleared at that time. For more information, refer to the “Managing Automatic Congestion Control” section on page 3-75.

### Corrective Action

If this alarm is caused by a rare spike in traffic, corrective action is not necessary. If this alarm occurs regularly, you should ensure that your links and routes are properly configured for load sharing, as described in the “SS7 Load Sharing Malfunction” section on page 8-52, and re-route some of your traffic to other Cisco MGCs.



#### Note

This alarm can occur when a provisioning session is active during peak busy hours. If this should happen, the alarm can be cleared by stopping the provisioning session. For more information on the MML commands to manage a provisioning session, refer to the “Provisioning your Cisco MGC” section on page 3-63.

---

## OverloadLight

This alarm occurs when the system has reached the threshold for overload level 1. A percentage of new calls, based on the call rejection percentage setting for overload level 1, are rejected until the abate threshold for overload level 1 is reached. This alarm is automatically cleared at that time. For more information, refer to the “Managing Automatic Congestion Control” section on page 3-75.

### Corrective Action

If this alarm is caused by a rare spike in traffic, corrective action is not necessary. If this alarm occurs regularly, you should ensure that your links and routes are properly configured for load sharing, as described in the “SS7 Load Sharing Malfunction” section on page 8-52, and re-route some of your traffic to other Cisco MGCs.



#### Note

This alarm can occur when a provisioning session is active during peak busy hours. If this should happen, the alarm can be cleared by stopping the provisioning session. For more information on the MML commands to manage a provisioning session, refer to the “Provisioning your Cisco MGC” section on page 3-63.

## PC UNAVAIL

This alarm occurs when a destination point code (DPC) is unavailable. This can be due to a network failure causing the DPC to become isolated, a local failure equipment failure causing a loss of connectivity, or a local provisioning failure causing the DPC or routes to it to be configured improperly.

### Corrective Action

To correct the problem identified by this alarm, perform the following steps:

- 
- Step 1** Other alarms associated indicating problems with hardware, the SS7 links, or the network should also be displayed. Resolve those alarms first.
- If resolving those alarms does not clear this alarm, proceed to Step 2.
- Step 2** Ensure that the provisioning settings for the DPC and for all routes to the DPC and adjacent STPs match the settings used on the far-end, as described in the “Retrieving Provisioning Data” section on page 3-67.
- If the configuration data associated with the DPC is incorrect, begin a dynamic reconfiguration session, as described in the “Invoking Dynamic Reconfiguration” section on page 3-65.
- If the configuration data associated with the DPC is correct, then proceed to Step 3.
- Step 3** Contact the Cisco TAC to further analyze the problem and determine a solution. For more information about contacting the Cisco TAC, refer to the “Obtaining Technical Assistance” section on page xviii.
- 

## Peer IP Links Failure

This alarm occurs when the IP links to the peer Cisco MGC are removed or down.

**Corrective Action**

To correct the problem identified by this alarm, perform the following steps:

- 
- Step 1** Verify that the Ethernet interfaces for the active and standby Cisco MGCs are working properly.



**Note** Information on verifying the proper operation of an Ethernet interface on the Cisco MGC host can be found in the Sun Microsystems documentation that came with your system.

---

If an element of the Ethernet connection (such as a cable or an Ethernet interface card) is not working properly, replace it. Otherwise, proceed to Step 2.



**Note** Information on removing and replacing an Ethernet interface card on the Cisco MGC host can be found in the Sun Microsystems documentation that came with your system.

---

- Step 2** Contact the Cisco TAC to further analyze the problem and determine a solution. For more information about contacting the Cisco TAC, refer to the “Obtaining Technical Assistance” section on page xviii.
- 

**PEER LINK A FAILURE**

This alarm occurs either because a communication path between peer modules was lost or a peer module has stopped communicating.

**Corrective Action**

To correct the problem identified by this alarm, perform the procedure in the “Resolving a Failed Connection to a Peer” section on page 8-125.

**PEER LINK B FAILURE**

This alarm occurs either because a communication path between peer modules was lost or a peer module has stopped communicating.

**Corrective Action**

To correct the problem identified by this alarm, perform the procedure in the “Resolving a Failed Connection to a Peer” section on page 8-125.

**PEER MODULE FAILURE**

This alarm occurs when communications to a peer module are lost, indicating failure.

**Corrective Action**

To correct the problem identified by this alarm, perform the procedure in the “Resolving a Failed Connection to a Peer” section on page 8-125.

## POM INACTIVITY TIMEOUT

This alarm occurs when the current provisioning session had been idle for 20 minutes without input any provisioning commands. If there is still no provisioning activity within the next five minutes, the session is terminated.

### Corrective Action

To correct the problem identified by this alarm, enter some provisioning MML commands, or stop the provisioning session as described in the “Saving and Activating your Provisioning Changes” section on page 3-64. For more information about provisioning your Cisco MGC, refer to the *Cisco Media Gateway Controller Software Release 7 Provisioning Guide*.

## POM SESSION TERMINATE

This alarm occurs when a provisioning session is terminated. Any additional provisioning commands are not accepted.

### Corrective Action

If you want to restart your provisioning session, perform the steps listed in the “Starting a Provisioning Session” section on page 3-63, using the same source version set equal to the destination version name.

## POM: DynamicReconfiguration

This alarm occurs when a dynamic reconfiguration procedure is started. It is cleared once the dynamic reconfiguration is successfully completed. Refer to the “Invoking Dynamic Reconfiguration” section on page 3-65 for more information.

### Corrective Action

If necessary, you can clear the alarm, as described in the “Clearing Alarms” section on page 8-4, or you can complete the dynamic reconfiguration procedure, as described in the “Invoking Dynamic Reconfiguration” section on page 3-65.

## POM: PEER\_SYNC\_ERR

This alarm occurs when the standby Cisco MGC attempts to synchronize the contents of its configuration library while a provisioning session is in progress on the active Cisco MGC.

### Corrective Action

To correct the problem identified by this alarm, either stop the provisioning session as described in the “Ending a Provisioning Session Without Activating your Changes” section on page 3-65, or save and activate your changes as described in the “Saving and Activating your Provisioning Changes” section on page 3-64.

## PRI: B-Channel not available

This alarm occurs when the Cisco MGC has received a PRI “setup” message, and the requested B channel is not available or cannot be allocated to the call.

## Corrective Action

If necessary, you can clear the alarm, as described in the “Clearing Alarms” section on page 8-4, or you can save and activate your provisioning session, as described in the “Saving and Activating your Provisioning Changes” section on page 3-64.

## ProcM No Response

The process manager is not responding to state information changes from the failover daemon.

## Corrective Action

To correct the problem identified by this alarm, perform the following steps:

- 
- Step 1** Stop the Cisco MGC software on the standby Cisco MGC, as described in the “Shutting Down the Cisco MGC Software Manually” section on page 2-4.
  - Step 2** Restart the Cisco MGC software on the standby Cisco MGC, as described in the “Starting the Cisco MGC Software” section on page 2-2.
  - Step 3** Perform a manual switchover, as described in the “Performing a Manual Switchover” section on page 3-80.
  - Step 4** Stop the Cisco MGC software on the newly standby Cisco MGC, as described in the “Shutting Down the Cisco MGC Software Manually” section on page 2-4.
  - Step 5** Restart the Cisco MGC software on the newly standby Cisco MGC, as described in the “Starting the Cisco MGC Software” section on page 2-2.
- 

## REPL: all connections failure

This alarm occurs when the Cisco MGC cannot establish communication to the peer Cisco MGC.

## Corrective Action

To correct the problem identified by this alarm, perform the following steps:

- 
- Step 1** Verify that the Ethernet interfaces for the Cisco MGC are working properly.



**Note** Information on verifying the proper operation of an Ethernet interface on the Cisco MGC host can be found in the Sun Microsystems documentation that came with your system.

---

If an element of the Ethernet connection (such as a cable or an Ethernet interface card) is not working properly, replace it. Otherwise, proceed to Step 2.



**Note** Information on removing and replacing an Ethernet interface card on the Cisco MGC host can be found in the Sun Microsystems documentation that came with your system.

---

- Step 2** Verify the replicator configuration on the Cisco MGCs, as described in the “Verifying Proper Configuration of Replication” section on page 8-123.



If that does not resolve the alarm, proceed to Step 3.

- Step 3** Contact the Cisco TAC to further analyze the problem and determine a solution. For more information about contacting the Cisco TAC, refer to the “Obtaining Technical Assistance” section on page xviii.
- 

## RSET CONFIG FAIL

This alarm occurs when the provisioning data for the SS7 route set to a DPC has invalid or incompatible parameter values. This does not occur due to a mismatch between the network topology and the DPC data.

### Corrective Action

To correct the problem identified by this alarm, perform the following steps:

- 
- Step 1** Ensure that the provisioning settings for the DPC and for all routes to the DPC match the settings used on the far-end, as described in the “Retrieving Provisioning Data” section on page 3-67.
- If the configuration data associated with the DPC is incorrect, begin a dynamic reconfiguration session, as described in the “Invoking Dynamic Reconfiguration” section on page 3-65.
- If the configuration data associated with the DPC is correct, then proceed to Step 3.
- Step 2** Contact the Cisco TAC to further analyze the problem and determine a solution. For more information about contacting the Cisco TAC, refer to the “Obtaining Technical Assistance” section on page xviii.
- 

## SC CONFIG FAIL

This alarm occurs when the provisioning parameters for the data link layer of a signaling channel are inconsistent or invalid. The signaling channel may already be provisioned. The configuration file might be corrupted and cannot be read by the system.

### Corrective Action

To correct the problem identified by this alarm, perform the following steps:

- 
- Step 1** Place the affected signaling channel in the out-of-service state, as described in the “Setting the Service State of a Signaling Channel” section on page 8-58.
- Step 2** Start a provisioning session, as described in the “Starting a Provisioning Session” section on page 3-63.
- Step 3** Remove the affected signaling channel from your configuration using the **prov-dlt** MML command. Refer to the *Cisco Media Gateway Controller Software Release 7 MML Command Reference Guide* for more information.
- Step 4** Referring to your local provisioning parameters, re-provision the signaling channel using the **prov-add** MML command. Refer to the *Cisco Media Gateway Controller Software Release 7 MML Command Reference Guide* for more information.
- Step 5** Save and activate your provisioning session, as described in the “Saving and Activating your Provisioning Changes” section on page 3-64.

- Step 6** Place the signaling channel in the in-service state, as described in the “Setting the Service State of a Signaling Channel” section on page 8-58.
- If that does not resolve the problem, proceed to Step 8.
- Step 7** Contact the Cisco TAC to further analyze the problem and determine a solution. For more information about contacting the Cisco TAC, refer to the “Obtaining Technical Assistance” section on page xviii.
- 

## SC FAIL

This alarm occurs when the signaling channel is down and unable to process traffic. As a result, the signaling channel is failing to negotiate a D-channel session, automatic restarts are not able to recover the session, and the data link-layer has failed. This can occur when SS7 SLTM/SLTA fails or when a PRI D-channel fails.

### Corrective Action

To correct the problem identified by this alarm, perform the following steps:

- 
- Step 1** Ensure that the near-end and far-end data link terminations are operating.
- If the near-end or far-end data link terminations are not operating, fix as necessary.
- If the near-end and far-end data link terminations are operating, proceed to Step 2.
- Step 2** Ensure that the provisioning settings for the signaling channel match the settings used on the far-end, as described in the “Retrieving Provisioning Data” section on page 3-67.
- If the configuration data for the signaling channel is incorrect, begin a dynamic reconfiguration session, as described in the “Invoking Dynamic Reconfiguration” section on page 3-65.
- If the configuration data for the signaling channel is correct, then proceed to Step 3.
- Step 3** Contact the Cisco TAC to further analyze the problem and determine a solution. For more information about contacting the Cisco TAC, refer to the “Obtaining Technical Assistance” section on page xviii.
- 

## SC M-OOS

This alarm occurs when the signaling channel has been manually set to the out of service state.

### Corrective Action

To correct the problem identified by this alarm, return the signaling channel to the in-service state as described in the “Setting the Service State of a Signaling Channel” section on page 8-58.

## srcpAudit: GwBackhaulProto

This alarm occurs when the returned backhaul protocol is different from what the Cisco MGC expects, which is a value of none. A mismatch here might cause minimal, partial, or complete signaling/call-control failure.

**Corrective Action**

To correct the problem identified by this alarm, perform the procedure in the “Resolving an SRCP Audit Alarm” section on page 8-97.

**srcpAudit: GwBackhaulSes**

This alarm occurs when the number of backhaul sessions is different from what the Cisco MGC expects. The Cisco MGC is expecting the value to match the provisioned value. Each backhaul session to the same IP address as the SRCP counts as 1. Some signaling information might be lost, leading to lost or failed calls.

**Corrective Action**

To correct the problem identified by this alarm, perform the procedure in the “Resolving an SRCP Audit Alarm” section on page 8-97.

**srcpAudit: GwControlProto**

This alarm occurs when the control protocol is different from what the Cisco MGC expects, which is a value of MGCP. A mismatch here might cause minimal, partial, or complete signaling failure.

**Corrective Action**

To correct the problem identified by this alarm, perform the procedure in the “Resolving an SRCP Audit Alarm” section on page 8-97.

**srcpAudit: GwCoordProto**

This alarm occurs when the coordination protocol is different from what the Cisco MGC expects, which is a value of SRCP 1.0. A mismatch here might cause alarms to be raised erroneously.

**Corrective Action**

To correct the problem identified by this alarm, perform the procedure in the “Resolving an SRCP Audit Alarm” section on page 8-97.

**srcpAudit: GwCulpAddr**

This alarm occurs when the IP address of the media gateway (CU) reported by the media gateway is different from that configured in the Cisco MGC. The Cisco MGC is expecting the IP address to match the value provisioned for the remote IP address entry of the signaling channel path. This can lead to a communication failure by the control protocol.

**Corrective Action**

To correct the problem identified by this alarm, perform the procedure in the “Resolving an SRCP Audit Alarm” section on page 8-97.

## srcpAudit: GwCulpPort

This alarm occurs when the value of the IP port reported by the media gateway (CU) is different from that configured in the Cisco MGC. The Cisco MGC is expecting the IP port to match the provisioned value for the remote port entry for this signaling channel or signaling service. This can lead to a communications failure by the control protocol.

### Corrective Action

To correct the problem identified by this alarm, perform the procedure in the “Resolving an SRCP Audit Alarm” section on page 8-97.

## srcpAudit: GwNumOfLines

This alarm occurs when the number of lines in the media gateway partition is different from what the Cisco MGC expects. The Cisco MGC is expecting the number of lines to match the value provisioned for the total number of bearer lines associated with this signaling service. This may affect service if a call are made on nonexistent lines. Another error should be raised elsewhere in the system if a call is placed to a nonexistent line.

### Corrective Action

To correct the problem identified by this alarm, perform the procedure in the “Resolving an SRCP Audit Alarm” section on page 8-97.

## srcpAudit: GwSlotNum

This alarm occurs when the hardware for the media gateway is in a different slot than the Cisco MGC expects, which is a value of 0. This should not affect service but might be an issue in hardware troubleshooting.

### Corrective Action

To correct the problem identified by this alarm, perform the procedure in the “Resolving an SRCP Audit Alarm” section on page 8-97.

## srcpAudit: GwSulpAddr

This alarm occurs when the IP address of the call agent (SU or MGC) reported by the media gateway is different from that configured in the Cisco MGC. The Cisco MGC is expecting the IP address to match the value provisioned for the local IP address entry for this signaling channel or signaling service. This can lead to a communications failure by the control protocol.

### Corrective Action

To correct the problem identified by this alarm, perform the procedure in the “Resolving an SRCP Audit Alarm” section on page 8-97.

## srcpAudit: GwSulpPort

This alarm occurs when the IP port of the call agent (SU or Cisco MGC) reported by the media gateway is different from that configured in the Cisco MGC. The Cisco MGC is expecting the IP port value to match the value provisioned for the local port entry for this signaling channel or signaling service. This can lead to a communications failure by the control protocol.

### Corrective Action

To correct the problem identified by this alarm, perform the procedure in the “Resolving an SRCP Audit Alarm” section on page 8-97.

## srcpAudit: GwType

This alarm occurs when the media gateway is of a different type than the Cisco MGC expects, which is a value of VISM. This may or may not affect service depending on whether the Cisco MGC has media gateway-specific coding.

### Corrective Action

To correct the problem identified by this alarm, perform the procedure in the “Resolving an SRCP Audit Alarm” section on page 8-97.

## srcpAudit: LineCoding

This alarm occurs when the line coding used by the media gateway for that line is different from that configured in the Cisco MGC for that line, which is a value of Unknown. This might lead to corrupted data on the B-channels.

### Corrective Action

To correct the problem identified by this alarm, perform the procedure in the “Resolving an SRCP Audit Alarm” section on page 8-97.

## srcpAudit: LineLoopback

This alarm occurs when the line loopback for that line used by the media gateway is different from that configured in the Cisco MGC for that line, which is a value of n. A line may be in a loopback state when the Cisco MGC believes it is available.

### Corrective Action

To correct the problem identified by this alarm, perform the procedure in the “Resolving an SRCP Audit Alarm” section on page 8-97.

## srcpAudit: LineSigProto

This alarm occurs when the signaling protocol used by the media gateway for that line is different from that configured in the Cisco MGC for that line. The Cisco MGC is expecting the signaling type associated with the backhaul signaling to the same remote IP address as the SRCP for this signaling channel. Some signaling information might be lost, leading to lost or failed calls.

**Corrective Action**

To correct the problem identified by this alarm, perform the procedure in the “Resolving an SRCP Audit Alarm” section on page 8-97.

**srcpAudit: LineState**

This alarm occurs when the line state for the line used by the media gateway is different from that configured in the Cisco MGC for that line, which is a value of e. A line might be disabled by the media gateway when the Cisco MGC believes it is available.

**Corrective Action**

To correct the problem identified by this alarm, perform the procedure in the “Resolving an SRCP Audit Alarm” section on page 8-97.

**SSN FAIL**

This alarm occurs when the SCP located by subsystem number (SSN) is not available.

**Corrective Action**

To correct the problem identified by this alarm, perform the following steps:

- 
- |               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|---------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | <p>Ensure that the provisioning settings for the SSN and the associated routes match the settings used on the far-end, as described in the “Retrieving Provisioning Data” section on page 3-67.</p> <p>If the configuration data associated with the SSN is incorrect, begin a dynamic reconfiguration session, as described in the “Invoking Dynamic Reconfiguration” section on page 3-65.</p> <p>If the configuration data associated with the SSN is correct, then proceed to Step 2.</p> |
| <b>Step 2</b> | <p>Verify the network configuration to confirm that the SCP identified with the SSN is reachable.</p> <p>If the SCP is not reachable, begin a dynamic reconfiguration session, as described in the “Invoking Dynamic Reconfiguration” section on page 3-65, and reprovision your data for an SCP that is reachable, or remove the SSN and its associated data.</p> <p>If the SCP is reachable, proceed to Step 3.</p>                                                                         |
| <b>Step 3</b> | <p>Contact the Cisco TAC to further analyze the problem and determine a solution. For more information about contacting the Cisco TAC, refer to the “Obtaining Technical Assistance” section on page xviii.</p>                                                                                                                                                                                                                                                                               |
- 

**Standby Warm Start**

This alarm occurs on the active Cisco MGC when a warm start process begins in the IOCM. This alarm clears automatically when the warm start process completes successfully. This alarm also occurs on the standby Cisco MGC when the **prov-sync** MML command is entered on the active Cisco MGC. In that case, the alarm clears automatically when the synchronization of provisioning data is complete.

### Corrective Action

Corrective action is only required when the alarm does not clear automatically. If this alarm does not clear automatically, verify that the `pom.dataSync` parameter in the `XECfgParm.dat` is set to *true* on each host, using the procedure in the “Rebooting Software to Modify Configuration Parameters” section on page 8-125.

## SUPPORT FAILED

This alarm occurs when the identified entity cannot provide service because a supporting entity is not providing service. The supporting entity may be hardware or software.

### Corrective Action

To correct the problem identified by this alarm, perform the following steps:

- 
- |               |                                                                                                                                                                                                                                                                                                       |
|---------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | Check for other alarms, as described in the “Retrieving All Active Alarms” section on page 8-3, that further identify the failed entity.                                                                                                                                                              |
| <b>Step 2</b> | Once you have identified the failed entity, replace it and restore it to service. If the entity is hardware, refer to the appropriate documentation for replacement. If it is software, attempt to reboot the software. If the alarms clear, the procedure is complete. Otherwise, proceed to Step 3. |
| <b>Step 3</b> | Contact the Cisco TAC to further analyze the problem and determine a solution. For more information about contacting the Cisco TAC, refer to the “Obtaining Technical Assistance” section on page xviii.                                                                                              |
- 

## SwitchoverFail

This alarm occurs when a switchover operation from the active Cisco MGC to the standby Cisco MGC has failed.

### Corrective Action

To correct the problem identified by this alarm, perform the procedure in the “Recovering from a Switchover Failure” section on page 8-113.

## XE Rsrc Fail

This alarm occurs when memory resources have been exhausted on the active Cisco MGC host. If this alarm occurs frequently you may need to add additional memory to your Cisco MGC. Refer to the Sun Microsystems documentation for your Cisco MGC host for more information about adding additional memory.

### Corrective Action

To correct the problem identified by this alarm, perform the following steps:

- 
- |               |                                                                                                         |
|---------------|---------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | Perform a manual switchover, as described in the “Performing a Manual Switchover” section on page 3-80. |
|---------------|---------------------------------------------------------------------------------------------------------|

- Step 2** Stop the Cisco MGC software on the newly standby Cisco MGC, as described in the “Shutting Down the Cisco MGC Software Manually” section on page 2-4.
- Step 3** Restart the Cisco MGC software on the newly standby Cisco MGC, as described in the “Starting the Cisco MGC Software” section on page 2-2.
- 

## SS7 Network Related Problems

The Cisco MGC node is considered to be a standard Service Switching Point (SSP) in an SS7 network. The SS7 network carries two types of signals:

- Circuit-related
- Noncircuit-related

The signals involved in the setup and teardown of bearer circuits are circuit-related. Non-circuit-related signals are used for all the ancillary services provided by the SS7 network, including database access and network management.

The SS7 protocol is composed of several levels or “parts,” including the following:

- Message Transfer Part (MTP)—Levels 1 (MTP1) through 3 (MTP3)
- Signaling Connection Control (SCCP)
- Application Service Part (ASP)
- Transaction Capabilities Application Part (TCAP)
- Telephony User Part (TUP)
- ISDN User Part (ISUP)
- Broadband ISUP (BISUP)

There are many variations of different parts of the SS7 protocol stack. MTP has ANSI, ITU, Bellcore, and a number of national variations. Each country and each major carrier may have slightly different variations of a part to fit its particular needs.

The SS7 network needs to have the highest degree of reliability. Each switch with access to the SS7 network must be configured to a preconceived set of network parameters. There is some risk that the person configuring a switch will not use the correct set of parameters or values. This is the root cause of most SS7 problems at both the MTP layers and upper layers of the SS7 protocol. A single parameter value, such as an incorrect timer value, can cause SS7 connectivity to act improperly or fail completely.

The first, and most important, step in troubleshooting SS7 related problems is to understand, and fully document, the SS7 network topology and protocols. The protocol documents are used as a reference over the months and years of maintenance on the SS7 network.

Troubleshooting SS7 network problems is described in the following sections:

- Signaling Channel Problems, page 8-51
- Signaling Destination Problems, page 8-55
- SS7 Network Troubleshooting Procedures, page 8-58



## Signaling Channel Problems

The Cisco MGC software generates signaling alarms if it detects problems with the transportation of data on a signaling channel or at a signaling destination.

Signaling alarms have four classifications of severity:

- Critical
- Major
- Minor
- Informational

**Note**

Multiple alarms are likely to occur for severe failures. For example, SUPPORT FAIL and SC FAIL would typically occur with LIF LOS.

Signaling links are the dedicated communication channels that the Cisco MGC uses to transfer signaling information among itself, the Cisco SLTs, and the Signal Transfer Points (STPs). Signaling links provide the necessary delivery reliability for higher-layer SS7 signaling protocols.

You can use the Cisco MGC software and MML commands to manage signaling channels and lines. You can retrieve signaling channel attributes, change the states of signaling channels, and change the state of signaling lines. See Chapter 3, “Cisco MGC Node Operations,” for detailed information.

**Note**

For more information on MML commands, refer to the *Cisco Media Gateway Controller Software Release 7 MML Reference Guide*.

Because all types of signaling channels have basically the same functionality, they are managed similarly. Unless otherwise noted, all commands, counters, and alarms mentioned here are applicable to all types of signaling channels.

Signaling channel problems are described in the following sections:

- SS7 Link is Out-of-Service, page 8-51
- SS7 Load Sharing Malfunction, page 8-52
- Physical Layer Failures, page 8-54
- Configuration Errors, page 8-54
- Supporting Entity Failures, page 8-54
- Incomplete Signaling, page 8-54
- Changing Service States, page 8-55

### SS7 Link is Out-of-Service

If an SS7 link is out-of-service on your system, perform the following steps:

**Step 1** Change the service state of the SS7 link to in-service, as described in the “Setting the Service State of a Link or Linkset” section on page 8-60.

If the SS7 link returns to service, the procedure is complete. Otherwise, proceed to Step 2.

**Step 2** If your system is using I/O cards to terminate the SS7 link, proceed to Step 3.

If your system is using Cisco SLTs to terminate the SS7 link, proceed to Step 4.

- Step 3** Verify that MTP1 is working correctly on the affected I/O card by checking for the following indications:
- Check the alarm LEDs on the affected I/O card. Dual green LEDs indicate that MTP1 is working correctly. Red or yellow LEDs indicate LOS, LOF and other errors.  
If both LEDs are green proceed to Step 5. Otherwise, proceed to Step 3b.
  - Check for LIF alarms for the affected I/O card, as described in the “Retrieving All Active Alarms” section on page 8-3.  
Perform the corrective actions for the alarm. These can be found in the “Alarm Troubleshooting Procedures” section on page 8-8.  
Repeat Step 1. If the link returns to service, the procedure is complete. Otherwise, proceed to Step 4.
- Step 4** Verify that MTP1 is working correctly on the affected Cisco SLT, as described in the “Identifying MTP1 Communication Problems” section on page B-11.  
If MTP1 is working correctly on the affected Cisco SLT, proceed to Step 6. Otherwise, correct the MTP1 problems as described in the “Resolving MTP1 Communication Problems” section on page B-11.  
Repeat Step 1. If the link returns to service, the procedure is complete. Otherwise, proceed to Step 6.
- Step 5** Verify that MTP2 is working correctly on the Cisco MGC by searching for excessive SUREM/AERM errors and link failure messages in the active system log file, as described in the “Viewing System Logs” section on page 8-4.  
If MTP2 is working correctly on the Cisco MGC, proceed to Step 8. Otherwise, correct the MTP2 problems as described in the “Resolving MTP1 Communication Problems” section on page B-11.  
Repeat Step 1. If the link returns to service, the procedure is complete. Otherwise, proceed to Step 8.
- Step 6** Verify that MTP2 is working correctly on the affected Cisco SLT, as described in the “Identifying MTP2 Communication Problems” section on page B-12.  
If MTP2 is working correctly on the affected Cisco SLT, proceed to Step 7. Otherwise, correct the MTP2 problems as described in the “Resolving MTP2 Communication Problems” section on page B-12.  
Repeat Step 1. If the link returns to service, the procedure is complete. Otherwise, proceed to Step 7.
- Step 7** Troubleshoot the SS7 link by performing the procedures found in the “Troubleshooting SS7 Link Problems” section on page B-4.  
If no problems can be found, proceed to Step 8. Otherwise, repeat Step 1. If the link returns to service, the procedure is complete. Otherwise, proceed to Step 8.
- Step 8** Contact the Cisco TAC to further analyze the problem and determine a solution. For more information about contacting the Cisco TAC, refer to the “Obtaining Technical Assistance” section on page xviii.
- 

## SS7 Load Sharing Malfunction

If load sharing on your SS7 links and/or routes is not working properly, perform the following steps:

- Step 1** Log in to the active Cisco MGC, start an MML session, and enter the following command to verify the priority settings of your SS7 links:
- ```
prov-rtrv:c7iplnk:"all"
```

The system returns a response similar to the following:

```
MGC-02 - Media Gateway Controller 2001-07-24 12:11:44
M RTRV
"session=active:c7iplnk"
/*
NAME          LNKSET          IF          IPADDR          PORT
PEERADDR      PRI          SLC          TIMESLOT      NEXTHOP          NETMASK
-----
-----
ls1lnk1          ls1          enif1          IP_Addr1          7000
172.24.200.9      1          0          0          0.0.0.0          255.255.255.255
ls2lnk1          ls2          enif1          IP_Addr1          7000
172.24.200.9      1          0          1          0.0.0.0          255.255.255.255
ls1lnk2          ls1          enif1          IP_Addr1          7000
172.24.200.10     1          1          0          0.0.0.0          255.255.255.255
ls2lnk2          ls2          enif1          IP_Addr1          7000
172.24.200.10     1          1          1          0.0.0.0          255.255.255.255
lk-3             ls-itu          enif1          IP_Addr1          7001
172.24.237.254    1          0          2          0.0.0.0          255.255.255.255
*/
```

The PRI field in the response shows the priority settings for your SS7 links. For load sharing to work properly, the priority settings for all of your links should be set to 1.

Step 2 Enter the following command to verify the priority settings of your SS7 routes:

```
prov-rtrv:ss7route:"all"
```

The system returns a response similar to the following:

```
MGC-02 - Media Gateway Controller 2001-07-24 12:25:05
M RTRV
"session=active:ss7route"
/*
NAME          OPC          DPC          LNKSET          PRI
-----
route1          opc1          dpc1          ls1          1
rout2          opc1          dpc2          ls2          1
rt3             opc2          scp2          ls-itu          1
rt1             opc2          stp1          ls-itu          1
rt2             opc2          scp1          ls-itu          1
*/
```

The PRI field in the response shows the priority settings for your SS7 routes. For load sharing to work properly, the priority settings for all of your routes should be set to 1.

Step 3 Start a provisioning session, as described in “Starting a Provisioning Session” section on page 3-63.

Step 4 If any of the SS7 links show a priority other than 1, you must change the priority settings to ensure proper link load sharing. Before you can change the priority settings for the link, you must take the link out-of-service, as described in the “Setting the Service State of a Link or Linkset” section on page 8-60.

Step 5 Modify the priority settings of the link by entering the following command:

```
prov-ed:c7iplnk:name="lnkname",pri=1
```

Where *lnkname* is the name of an SS7 link that does not have a priority of 1.

Repeat this step for each link that does not have a priority of 1.

Step 6 If any of the SS7 routes show a priority other than 1, you must change the priority settings to ensure proper route load sharing. Before you can change the priority settings for the route, you must take the route out-of-service, as described in the “Setting the Service State of a Signaling Point Code” section on page 8-60.

Step 7 Modify the priority settings of the link by entering the following command:

```
prov-ed:ss7route:name="rtname",pri=1
```

Where *rtname* is the name of an SS7 route that does not have a priority of 1.

Repeat this step for each route that does not have a priority of 1.

Step 8 Save and activate your provisioning changes, as described in the “Saving and Activating your Provisioning Changes” section on page 3-64.

Physical Layer Failures

The major issues with the physical layer of an SS7 signaling link are related to cabling, clock source, and connector pinouts. The cable should be of high quality (shielded) and the connectors should be attached and crimped solidly. Since SS7 links are synchronous, one side of the link must provide the clock source and the other side must use this clock signal to read the bits.

Finally, the most common mistake is to use the wrong cable pinouts for a specific physical configuration. Make sure that the connector has the correct number of pins (RJ-45, DB-25) and that each pin maps to the correct signal. A number of different physical layers are supported, including ANSI T1, CEPT E1, and V.35. Make sure that the cable complies with the connector and the physical protocol being used.

If the configuration appears to be valid and the cable pinout is good, check that the signal is being sent and received correctly. Use a Bit Error Rate Tester (BERT) or perform a signal loopback on the interface. It is possible that the cable is bad, so try to replace it. Finally, it is possible that the line card is bad, so you might try replacing it too.

Configuration Errors

The most common mistake in SS7 signal link configuration is to misconfigure the Signal Link Code (SLC) for the SS7 link. This is a preconfigured code on both ends of the link. If the SLC or the point codes do not match, the link does not align and no transmission can take place.

For T1 and E1 connectors, an SS7 signaling link is carried in a single 56- or 64-kbps time slot. The time slot that is used must also agree on both sides of the link.

Make sure the MTP2 timers and thresholds agree with the network defaults. Confirm that the far-end switch or STP has the same values as your system.

When a Cisco SLT is used to terminate MTP2, confirm that the RUDP parameters agree on both sides and are consistent with the documentation.

Supporting Entity Failures

An SS7 signaling link has a hierarchy of network element entities that must be functioning before the link can function. These include the physical interface (discussed above) and the control software for the link. If any of these fail, the link also fails.

Incomplete Signaling

Link failures between the Cisco SLT and the Cisco MGC can be caused by

- Ethernet card failure on the Cisco SLT

- Ethernet card failure on the LAN switch
- LAN switch failure
- Fast Ethernet interface card failure on the Cisco MGC

In each of the above cases, it is impossible to transfer MTP3 signaling messages from the Cisco SLT to the Cisco MGC. Cisco SLT platform failure (which is equivalent to MTP2 failure) causes signaling messages to be unable to go to MTP3. The MTP2 layer on the Cisco SLT is supposed to transmit SIPO messages to the STP mated pair to initiate the changeover procedure. Cisco SLT platform failure on the SS7 network is detected by the mated STP pair, which detects timer expiration and link unavailability.

Changing Service States

Signal channels comply with the Generic Service State model defined in the “Physical Layer Failures” section on page 8-54. You can change the desired service state of a signaling channel using the following transition requests. Note that there is a difference between a desired service state and an actual service state, and the Cisco MGC might not be able to honor the request. For example, a signal channel that is out-of-service due to an equipment failure cannot transition to an in-service state upon request. The Cisco MGC attempts to bring the channel in-service, but it fails. The failure must be fixed before the transition can succeed.

- In-service (IS)—The signaling channel is requested to start providing service.
- Out-of-service (OOS)—The signaling channel is requested to stop providing service.
For some protocols, this request is accepted, but not granted until after all calls have been released. During the interim period, the channel’s service state appears as OOS, PEND.
- Forced out-of-service (FOOS)—The signaling channel is requested to stop providing service immediately regardless of related call states, and to drop currently active calls.
- Inhibit (INH)—The signaling channel is requested to be put into an inhibit state. This state is for SS7 signaling channels only and fails on other types of signaling channels.
In this state, the channel is active but does not provide service for call processing. If the signaling channel is the last one in the signal path, the inhibit request is denied and an error is returned.
- Un-inhibit (UNH)—The signaling channel is requested to be removed from an INH state and to provide service for call processing. This state is for SS7 signaling channels only and fails on other types of signaling channels.
Use this option (UNH), rather than the IS option, to return an inhibited signaling channel to service.

**Note**

Changing the state of a signaling channel generates an alarm. For more information on retrieving and clearing alarms, see “Troubleshooting Using Cisco MGC Alarms” section on page 8-2

Signaling Destination Problems

Signaling destinations refer to the endpoints of a network. Typically, if signaling links are in service, the signaling destinations should also be in service.

For ISDN signaling, the signaling channel is in service if the Cisco MGC can talk to the media gateway and ISDN backhaul is configured. The destination is in service if the signaling channel is in service and the remote ISDN device is up.

Apparent mismatches can occur due to

- SS7 traffic restart handling (TRW/TRA)

- SS7 STP problems
- Configuration problems
- Software problems

An SS7 STP is treated as an adjacent point code (APC) to the Cisco MGC. SS7 MTP uses a message exchange called Signaling Link Test Message (SLTM)/Signaling Link Test Acknowledgment (SLTA) to confirm that the far-end point code is the one configured. The SLTM consists of the originating point code (OPC) of the Cisco MGC, an APC number, and an SS7 network indicator. If the values for these parameters match with the values used for these at the far-end switch, an SLTA is returned. If the value for any of these parameters do not match, the far-end switch does not send an SLTA. The Cisco MGC drops the link and tries to realign it. This process continues until the SLTM parameters match on both sides. The problem is manifested by the SS7 links dropping and recovering in roughly 30-second cycles (this is referred to as bouncing).

The following sections describe signaling destination problems:

- Bouncing SS7 Links, page 8-56
- Configuration Errors, page 8-57
- Traffic Restart, page 8-57
- SS7 Destination is Out of Service, page 8-57
- SS7 Route is Out of Service, page 8-57
- SS7 Destination is Unavailable, page 8-58

Bouncing SS7 Links

Usually, this condition is caused by mismatched signaling link codes (SLCs) or DPCs/OPCs between the Cisco MGC and the far end. To resolve a bouncing SS7 condition, perform the following steps:

-
- Step 1** Verify that the SLC, OPC, and DPC provisioning settings match with those used on the far end. To do this, enter the **prov-rtrv** MML command for the SS7 link, OPC, and DPC components, as described in the “Retrieving Provisioning Data” section on page 3-67, and compare the values found there with those used by the far end.
- If the provisioning settings for the SLC, OPC, and DPC match with those used on the far end, proceed to Step 2. Otherwise, modify the settings to match with those used on the far end. Refer to the “Invoking Dynamic Reconfiguration” section on page 3-65 for more information about modifying the settings of a provisioned component. If that clears the problem, the procedure is complete. Otherwise, proceed to Step 2.
- Step 2** Ensure that the local MTP3 timer settings match the network defaults by performing the “Verifying MTP3 Timers” section on page 8-63.
- If the local MTP3 timer settings match the network defaults, proceed to Step 3. Otherwise, contact the far-end to determine whether their timer settings can be changed to match your settings. If that clears the problem, the procedure is complete. Otherwise, proceed to Step 3.
- Step 3** View the system logs, as described in the “Viewing System Logs” section on page 8-4, looking for excessive alignment error monitoring (AERM) logs. If large numbers of AERM logs are present, proceed to Step 4. If no AERM logs are present, contact the Cisco TAC for assistance. Refer to the “Obtaining Technical Assistance” section on page xviii for more information about contacting the Cisco TAC.

- Step 4** Determine why the link is not aligning properly by checking the alignment status on the Cisco SLT associated with the affected link, as described in the “Verifying the Link Alignment Status” section on page B-6.
-

Configuration Errors

If the SS7 DPC is fully associated, it can have the same SLTM/SLTA problems as described above.

If the SS7 DPC is quasi-associated, the most common cause for failure is a route misconfiguration. Review the route information between the Cisco MGC and the DPC to make sure that the APCs are valid, the route priorities are set correctly, and the route uses the appropriate linkset.

Traffic Restart

Make sure that the MTP3 traffic restart timers and thresholds agree with the network defaults. Confirm that the far-end switch or STP also has the same values.

SS7 Destination is Out of Service

A signaling destination is typically out of service when all of the SS7 links from the Cisco MGC to the destination or APC are out of service, or when all of the SS7 links from the destination to the APC are out of service.

To restore an SS7 destination to service, perform the following steps:

-
- Step 1** Contact your SS7 provider and have them verify the links from the DPC to the associated STP.
- Step 2** Verify the state of the signaling channels, as described in the “Retrieving Signaling Channel Attributes” section on page 3-48.
- If any of the SS7 links are out-of-service, restore the links as described in the “SS7 Link is Out-of-Service” section on page 8-51. If all of the SS7 links to a destination are out-of-service, restore the destination as described in the “SS7 Destination is Out of Service” section on page 8-57.
-

SS7 Route is Out of Service

To restore an SS7 route to service, perform the following steps:

-
- Step 1** Change the service state of the destination to in-service, as described in the “Setting the Service State of a Destination” section on page 8-59.
- If the destination goes into service, the procedure is complete. Otherwise, proceed to Step 2.
- Step 2** Verify the state of the signaling channels, as described in the “Retrieving Signaling Channel Attributes” section on page 3-48.
- If none of the SS7 links are in-service, proceed to Step 3. If all or at least one of the SS7 links to the destination are in-service, then contact your SS7 provider and have them verify the links from the DPC to the associated STP.

- Step 3** Determine why the link is not aligning properly by checking the alignment status on the Cisco SLT associated with the affected link, as described in the “Verifying the Link Alignment Status” section on page B-6.
-

SS7 Destination is Unavailable

An SS7 destination is unavailable when all of the routes to the destination are out-of-service. Perform the procedure defined in the “SS7 Route is Out of Service” section on page 8-57.

SS7 Network Troubleshooting Procedures

The following sections are procedures used to resolve problems associated with the Cisco MGC node’s connection to the SS7 network:

- Setting the Service State of a Signaling Channel, page 8-58
- Setting the Service State of a Destination, page 8-59
- Setting the Service State of a Signaling Point Code, page 8-60
- Setting the Service State of a Link or Linkset, page 8-60
- Setting the Service State of a Local Subsystem Number, page 8-61
- Verifying MTP Timer Settings, page 8-61
- Modifying MTP Timer Settings, page 8-65
- Managing Japanese SS7 Signaling Link Tests, page 8-67
- Managing Japanese SS7 Signaling Route Tests, page 8-68
- Verifying Proper Loading of a Dial Plan, page 8-69

Setting the Service State of a Signaling Channel

To set the service state of a signaling channel or linkset, perform the following steps:

- Step 1** Log in to the active Cisco MGC, start an MML session, and enter the following command:

```
set-sc-state:sig_chan:serv_state
```

Where:

- *sig_chan*—The MML name of the desired signaling channel or linkset.
- *serv_state*—The desired service state. The valid states are listed below:
 - IS—Places a signaling channel or linkset in service. This state is valid for all signaling channel or linkset types.
 - OOS—Takes a signaling channel or linkset out of service. This state is valid for all signaling channel or linkset types.



Note You must use the FOOS option to set the last link of a linkset OOS.

- FOOS—Forces a signaling channel or linkset out of service. This state is valid for all signaling channel or linkset types.
- INH—Inhibits an SS7 link. This state is valid only for SS7 signaling links.
- UNH—Uninhibits an SS7 link. This state is valid only for SS7 signaling links.

For example, to set the service state of a signaling channel called `iplink1` to IS, enter the following command:

```
set-sc-state:iplink1:IS
```

- Step 2** Verify that the state of the signaling channel or linkset has changed by entering the **rtrv-sc** command, as described in the “Retrieving Signaling Channel Attributes” section on page 3-48.

Setting the Service State of a Destination

To set the service state of a destination, perform the following steps:



Caution

The **set-dest-state** command should only be used while you are dynamically reconfiguring the system. Do not use the **set-dest-state** command to take a signaling service out-of-service during a maintenance session, as all calls associated with the specified signaling service will be dropped. You should instead use the **blk-cic** command to block the CICs associated with the signaling service when you need to perform maintenance.

- Step 1** Log in to the active Cisco MGC, start an MML session, and enter the following command:

```
set-dest-state:dest:serv_state
```

Where:

- *dest*—The MML name of the desired destination, such as an SS7 point code, FAS signaling service, or IP FAS signaling service.
- *serv_state*—The desired service state. The valid states are listed below:
 - IS—Places a destination in service.
 - OOS—Takes a destination out of service.



Note

Before you can take a NAS signaling service out of service, you must shut down the D channel on the associated media gateway. Refer to the documentation for the media gateway for more information on shutting down D channels.

For example, to set the service state of a destination called `dpc1` to IS, enter the following command:

```
set-dest-state:dpc1:IS
```

- Step 2** Verify that the state of the destination has changed by entering the **rtrv-dest** command, as described in the “Retrieving Signaling Destination Service States” section on page 3-50.

Setting the Service State of a Signaling Point Code

To set the service state of a signaling point code, perform the following steps:



Caution

The **set-spc-state** command should only be used while you are dynamically reconfiguring the system. Do not use the **set-spc-state** command to take an SS7 signaling service out-of-service during a maintenance session, as all calls associated with the specified SS7 signaling service will be dropped. You should instead use the **blk-cic** command to block the CICs associated with the SS7 signaling service when you need to perform maintenance.

Step 1 Log in to the active Cisco MGC, start an MML session, and enter the following command:

```
set-spc-state:sig_pc:serv_state
```

Where:

- *sig_pc*—The MML name of the desired signaling point code.
- *serv_state*—The desired service state. The valid states are listed below:
 - IS—Places a signaling point code in service.
 - OOS—Takes a signaling point code out of service.

For example, to set the service state of signaling point code called stp1 to IS, enter the following command:

```
set-spc-state:stp1:IS
```

Step 2 Verify that the state of the signaling channel has changed by entering the **rtrv-spc** command, as described in the “Retrieving the State of Point Codes” section on page 3-51.

Setting the Service State of a Link or Linkset

To set the service state of a link or linkset, perform the following steps:

Step 1 Log in to the active Cisco MGC, start an MML session, and enter the following command:

```
set-lnk-state:lname:serv_state
```

Where:

- *lname*—The MML name of the desired link or linkset.
- *serv_state*—The desired service state. The valid states are listed below:
 - IS—Places a link or linkset in service.
 - OOS—Takes a link or linkset out of service.



Note

You must use the FOOS option to set the last link of a linkset OOS.

- FOOS—Forces a link or linkset out of service.
- INH—Inhibits a link or linkset.
- UNH—Uninhibits a link or linkset.

For example, to set the service state of a link called ls1-link1 to IS, enter the following command:

```
set-sc-state:ls1-link1:IS
```

- Step 2** Verify that the state of the link or linkset has changed by entering the **rtrv-link** command, as described in the “Retrieving the Service State of a Linkset” section on page 3-51.
-

Setting the Service State of a Local Subsystem Number

To set the service state of a local subsystem number (LSSN), perform the following steps:

- Step 1** Log in to the active Cisco MGC, start an MML session, and enter the following command:

```
set-lssn-state:ssn:serv_state
```

Where:

- *ssn*—The MML name of the desired LSSN.
- *serv_state*—The desired service state. The valid states are listed below:
 - IS—Places an LSSN in service.
 - OOS—Takes an LSSN out of service.

For example, to set the service state of an LSSN called lnp to IS, enter the following command:

```
set-lssn-state:lnp:IS
```

- Step 2** Verify that the state of the LSSN has changed by entering the **rtrv-lssn** command, as described in the “Retrieving the State of All Local Subsystem Numbers” section on page 3-53.
-

Verifying MTP Timer Settings

When resolving signaling problems between the Cisco MGC and an associated SS7 network element (such as an STP), you may need to verify that the MTP2 and MTP3 timer settings used by the Cisco MGC conform to settings used by the associated SS7 network element. MML commands are used to retrieve the settings for the MTP2 and MTP3 timers on the Cisco MGC. The following subsections describe methods for verifying the MTP timer settings on the Cisco MGC.



Note

Refer to the *Cisco Media Gateway Controller Software Release 7 Provisioning Guide* for more information on the MTP timers.

The procedure used to verify the settings for MTP2 timers varies based on how SS7 signaling is terminated for your Cisco MGC. If you are using Cisco SLTs to terminate SS7 signaling, refer to the “Verifying MTP2 Timers for Cisco SLTs” section on page 8-62. If you are using I/O cards to terminate SS7 signaling, refer to the “Verifying MTP2 Timers for I/O Cards” section on page 8-62. The procedure to verify MTP3 timers is the same for both SS7 signaling termination methods.

If you find, after you verify the settings, that you need to modify the settings for the MTP timers, proceed to the “Modifying MTP Timer Settings” section on page 8-65.

Verifying MTP2 Timers for Cisco SLTs

To verify the values used for the MTP2 timers when you are using Cisco SLTs to terminate SS7 signaling, complete the following steps:

- Step 1** Enter the following command at the Cisco SLT to display the settings for the MTP2 timers:

```
Router #show SS7 mtp2 timer channel
```

Where: *channel* specifies a channel, 0 through 3.

The system returns a message similar to the following:

```
SS7 MTP2 Timers for channel 0 in milliseconds
Protocol version for channel 0 is Japan NTT Q.703 Version 1-1
  T1 aligned/ready = 15000
    T2 not aligned = 5000
      T3 aligned = 3000
T4 Emergency Proving = 3000
  T4 Normal Proving = 3000
    T5 sending SIB = 200
      T6 remote cong = 3000
T7 excess ack delay = 2000
  T8 errored int mon = 0
TA SIE timer = 20
  TF FISU timer = 20
    TO SIO timer = 20
      TS SIOS timer = 20
```

- Step 2** Verify the MTP2 timers settings listed for the Cisco SLTs against the MTP2 timers used at the associated destination.

If the MTP2 timers settings match, your signaling problem has different cause. Continue troubleshooting the problem.

If the MTP2 timers settings do not match, perform the procedure in the “Modifying MTP2 Timers for Cisco SLTs” section on page 8-65.

Verifying MTP2 Timers for I/O Cards

To verify the values used for the MTP2 timers when you are using I/O cards to terminate SS7 signaling, complete the following steps:

- Step 1** Log on to active Cisco MGC, start an MML session, and enter the following command to display the settings for the MTP2 timers:



Note

If you use this command to verify the settings for the MTP2 timers when you are using Cisco SLTs to terminate SS7 signaling links, the displayed results reflect the default values for the SS7 variant assigned to the linkset, not the actual values used. Refer to the “Verifying MTP2 Timers for Cisco SLTs” section on page 8-62 for the procedure to obtain the actual settings used for these MTP2 timers.

```
prov-rtrv:signvcprop:name="protocol"
```

Where *protocol* is the MML name for the SS7 protocol family being used, such as SS7-ANSI or SS7-ITU.

The system returns a message similar to the following:

```
MGC-01 - Media Gateway Controller 2001-06-01 10:31:00
M   RTRV
    "session=active:lnksetprop"
    /*
mtp2AermEmgThr = 1
mtp2AermNrmThr = 4
mtp2CongDiscard = false
mtp2LssuLen = 1
mtp2MaxAlignRetries = 5
mtp2MaxMsuFrmLen = 272
mtp2MaxOutsFrames = 127
mtp2ProvingEmgT4 = 6
mtp2ProvingNormalT4 = 23
mtp2SuermThr = 64
mtp2T1 = 130
mtp2T2 = 115
mtp2T3 = 115
mtp2T5 = 1
mtp2T6 = 30
mtp2T7 = 10
mtp3ApcMtpRstrttT28 = 30
mtp3DlnkConnAckT7 = 10
mtp3FrcUnhT13 = 10
mtp3InhAckT14 = 20
mtp3LocInhTstT20 = 900
mtp3MaxSlTries = 2
mtp3MsgPriority = 2
mtp3MtpRstrttT24 = 100
mtp3RepeatRstrttT26 = 150
mtp3TfrUsed = false
mtp3TraSntT29 = 600
mtp3tstSlTmT1 = 60
mtp3tstSlTmT2 = 600
mtp3UnhAckT12 = 10
reference = ANSI92
rudpAck = enable
rudpKeepAlives = enable
rudpNumRetx = 2
rudpRetxTimer = 6
rudpSdm = enable
rudpWindowSz = 32
```

- Step 2** Verify the MTP2 timers settings listed for the I/O cards against the MTP2 timers used at the associated destination.

If the MTP2 timers settings match, your signaling problem has different cause. Continue troubleshooting the problem.

If the MTP2 timers settings do not match, perform the procedure in the “Modifying MTP2 Timers for I/O Cards” section on page 8-66.

Verifying MTP3 Timers

To verify the values used for the MTP3 timers, complete the following steps:

- Step 1** Log on to active Cisco MGC, start an MML session, and enter the following command to display the settings for the MTP3 timers:

```
prov-rtrv:sigsvccprop:name="protocol"
```

Where *protocol* is the MML name for the SS7 protocol family being used, such as SS7-ANSI or SS7-ITU.

The system returns a message similar to the following:

```
MGC-01 - Media Gateway Controller 2001-06-01 10:31:00
M   RTRV
    "session=active:lnksetprop"
    /*
mtp2AermEmgThr = 1
mtp2AermNrmThr = 4
mtp2CongDiscard = false
mtp2LssuLen = 1
mtp2MaxAlignRetries = 5
mtp2MaxMsuFrmLen = 272
mtp2MaxOutsFrames = 127
mtp2ProvingEmgT4 = 6
mtp2ProvingNormalT4 = 23
mtp2SuermThr = 64
mtp2T1 = 130
mtp2T2 = 115
mtp2T3 = 115
mtp2T5 = 1
mtp2T6 = 30
mtp2T7 = 10
mtp3ApcMtpRstrttT28 = 30
mtp3DlnkConnAckT7 = 10
mtp3FrcUnhT13 = 10
mtp3InhAckT14 = 20
mtp3LocInhTstT20 = 900
mtp3MaxSltTries = 2
mtp3MsgPriority = 2
mtp3MtpRstrttT24 = 100
mtp3RepeatRstrttT26 = 150
mtp3TfrUsed = false
mtp3TraSntT29 = 600
mtp3tstSltmT1 = 60
mtp3tstSltmT2 = 600
mtp3UnhAckT12 = 10
reference = ANSI92
rudpAck = enable
rudpKeepAlives = enable
rudpNumRetx = 2
rudpRetxTimer = 6
rudpSdm = enable
rudpWindowSize = 32
```

Step 2 Verify the MTP3 timers settings listed against the MTP3 timers used at the associated destination.

If the MTP3 timers settings match, your signaling problem has different cause. Continue troubleshooting the problem.

If the MTP3 timers settings do not match, perform the procedure in the “Modifying MTP3 Timers” section on page 8-66.

Modifying MTP Timer Settings

As of Release 7.4(12), you can modify the settings for the MTP timers. For more information, refer to the *Release Notes for the Cisco Media Gateway Controller Software*.

When resolving signaling problems between the Cisco MGC and an associated SS7 network element (such as an STP), you may need to modify the MTP2 and MTP3 timer settings on the Cisco MGC, so that they conform to the settings used by that SS7 network element. You use MML commands to modify the settings for the MTP2 and MTP3 timers. The following subsections describe methods for modifying the settings of the MTP timers on the Cisco MGC.

The procedure used to modify the settings for MTP2 timers varies based on how SS7 signaling is terminated for your Cisco MGC. If you are using Cisco SLTs to terminate SS7 signaling, refer to the “Modifying MTP2 Timers for Cisco SLTs” section on page 8-65. If you are using I/O cards to terminate SS7 signaling, refer to the “Modifying MTP2 Timers for I/O Cards” section on page 8-66. The procedure for modifying MTP3 timers is the same for both SS7 signaling termination methods.

**Note**

Refer to the *Cisco Media Gateway Controller Software Release 7 Provisioning Guide* for more information on the MTP timers.

You might want to verify the new settings after the modification is complete. To do this, refer to the procedure in the “Verifying MTP Timer Settings” section on page 8-61.

Modifying MTP2 Timers for Cisco SLTs

Use the following MML commands at the Cisco SLT to modify the settings for the MTP2 timers:

```
Router (config)#ss7 mtp-variant standard channel
Router(config-standard)# parameters
```

Where:

- *standard*—Name of the SS7 standards used for your links. Valid values are Bellcore, ITU, NTT, and TTC
- *channel*—Specifies a channel, 0 through 3
- *parameters*—The timer number and the new value for the timer

**Note**

Refer to the *Cisco Signaling Link Terminal* documentation for more information on the parameters for this command.

In the following example, the aligned/ready timer duration on channel 0 is set to 30,000 milliseconds:

```
Router(config)# ss7 mtp2-variant Bellcore 0
Router(config-Bellcore)# T1 30000
```

In the following example, the aligned/ready timer is restored to its default value of 13,000 milliseconds:

```
Router(config)# ss7 mtp2-variant Bellcore 0
Router(config-Bellcore)# no T1
```

You might want to verify the new settings after the modification is complete. To do this, refer to the procedure in the “Verifying MTP2 Timers for Cisco SLTs” section on page 8-62.

Modifying MTP2 Timers for I/O Cards

To modify the settings for the MTP2 timers when you are using I/O cards to provide SS7 signaling links, perform the following steps:

Step 1 Start a provisioning session as described in the “Starting a Provisioning Session” section on page 3-63.

Step 2 Modify the parameters for the desired MTP2 timers by entering the following command:

```
prov-ed:lnkset:name="protocol",param_name=param_value
```

Where:

- *protocol*—MML name for the SS7 protocol family being used, such as SS7-ANSI or SS7-ITU.
- *param_name*—Name of the MTP timer you want to change
- *param_value*—New value for the MTP timer



Note

Refer to the *Cisco Media Gateway Controller Software Release 7 Provisioning Guide* for more information on the parameters for this command.

In the following example, the MTP2 T2 timer, maximum period in a Not Aligned state before returning to an OOS state, is set to 120 tenths of a second:

```
prov-ed:lnkset:name="SS7-ANSI",mtp2T2=120
```

Step 3 Save and activate your provisioning session as described in the “Saving and Activating your Provisioning Changes” section on page 3-64.

Step 4 Reboot your system as described in the “Rebooting Your System to Modify Properties” section on page 8-124.

Modifying MTP3 Timers

To modify the settings for the MTP3 timers, perform the following steps:

Step 1 Start a provisioning session as described in the “Starting a Provisioning Session” section on page 3-63.

Step 2 Modify the parameters for the desired MTP3 timers by entering the following command:

```
prov-ed:lnkset:name="protocol",param_name=param_value
```

Where:

- *protocol*—MML name for the SS7 protocol family being used, such as SS7-ANSI or SS7-ITU.
- *param_name*—Name of the MTP timer you want to change
- *param_value*—New value for the MTP timer



Note

Refer to the *Cisco Media Gateway Controller Software Release 7 Provisioning Guide* for more information on the parameters for this command.

In the following example, the MTP3 T1 timer, waiting for signaling link test acknowledgment message, is set to 65 tenths of a second:

```
prov-ed:lnkset:name="SS7-ANSI",mtp3tstsltmT1=65
```

- Step 3** Save and activate your provisioning session as described in the “Saving and Activating your Provisioning Changes” section on page 3-64.
- Step 4** Reboot your system as described in the “Rebooting Your System to Modify Properties” section on page 8-124.
-

Managing Japanese SS7 Signaling Link Tests

The following subsections detail the procedures used to manage the tests that can be run on a signaling link configured for Japanese SS7:

- Starting an Japanese SS7 Signaling Link Test, page 8-67
- Retrieving Results for a Japanese SS7 Signaling Link Test, page 8-67

Starting an Japanese SS7 Signaling Link Test

To start a signaling link test on a link configured for Japanese SS7, log in to the active Cisco MGC, start an MML session, and enter the following command:

```
sta-ss7-slt:link
```

Where *link* is the MML name of a link configured for Japanese SS7.

For example, to start a signaling link test on a link called ls1-link1, you would enter the following command:

```
sta-ss7-slt:ls1-link1
```

Retrieving Results for a Japanese SS7 Signaling Link Test

To retrieve the results of a Japanese SS7 signaling link test, log in to the active Cisco MGC, start an MML session, and enter the following command:

```
rtrv-ss7-slt:link
```

Where *link* is the MML name of a link configured for Japanese SS7.

For example, to retrieve the results of a signaling link test run on a link called ls1-link1, you would enter the following command:

```
rtrv-ss7-slt:ls1-link1
```

The system returns a result that indicates the name of the link and the status of the signaling link test. The valid status responses are listed below:

- TEST PASSED
- TEST FAILED (reasons for failure may be any of the following:)
 - TEST TIMEOUT
 - LINK INACTIVE
 - LINKSET INACTIVE

- ROUTE UNAVAILABLE
- INVALID TEST PATTERN
- INVALID SLC
- FLOW CONTROL ON
- UNKNOWN REASON
- COMPLETED *hh:mm:ss*
- TEST RUNNING

For example, here is a sample response to a signaling link test run on a link called ls1-link1:

```
Media Gateway Controller - MGC-01 2000-01-12 15:18:41
M   RTRV
    "ls1link1:TEST PASSED; COMPLETED 15:18:34"
```

Managing Japanese SS7 Signaling Route Tests

The following subsections detail the procedures used to manage the tests that can be run on a signaling route configured for Japanese SS7:

- Starting a Japanese SS7 Signaling Route Test, page 8-68
- Retrieving Results for a Japanese SS7 Signaling Route Test, page 8-68

Starting a Japanese SS7 Signaling Route Test

To start a signaling route test on a route configured for Japanese SS7, log in to the active Cisco MGC, start an MML session, and enter the following command:

```
sta-ss7-srt:pt_code:lset="linkset"
```

Where:

- *pt_code*—MML name of an adjacent point code (APC) or destination point code (DPC) configured for Japanese SS7.
- *linkset*—MML name of a linkset associated with the specified destination.

For example, to start a signaling route test on a point code called dpc1 associated with a linkset called ls1, you would enter the following command:

```
sta-ss7-srt:dpc1:lset="ls1"
```

Retrieving Results for a Japanese SS7 Signaling Route Test

To retrieve the result of a Japanese SS7 signaling route test, log in to the active Cisco MGC, start an MML session, and enter the following command:

```
rtrv-ss7-srt:pt_code:lset="linkset"
```

Where:

- *pt_code*—MML name of an adjacent point code (APC) or destination point code (DPC) configured for Japanese SS7.
- *linkset*—MML name of a linkset associated with the specified destination.

For example, to retrieve the results of a signaling route test run on a point code called dpc1 associated with a linkset called ls1, you would enter the following command:

```
rtrv-ss7-srt:dpc1:ls1="ls1"
```

The system returns a result that indicates the name of the link and the status of the signaling route test. The valid status responses are listed below:

- TEST PASSED
- TEST FAILED (reasons for failure may be any of the following:)
 - TEST TIMEOUT
 - LINK INACTIVE
 - LINKSET INACTIVE
 - ROUTE UNAVAILABLE
 - INVALID TEST PATTERN
 - INVALID SLC
 - FLOW CONTROL ON
 - UNKNOWN REASON
- COMPLETED *hh:mm:ss*
- TEST RUNNING

For example, here is a sample response to a signaling route test run on a point code called dpc1 associated with a linkset called ls1:

```
Media Gateway Controller - MGC-01 2000-01-12 15:20:09
M RTRV
"dpc1:TEST FAILED; TEST TIMEOUT; COMPLETED 15:20:01"
```

Verifying Proper Loading of a Dial Plan

-
- Step 1** Search the active system log file, as described in the “Viewing System Logs” section on page 8-4, for logs that indicate that the dial plan was loaded incorrectly.
- If the dial plan was not loaded correctly, reload the dial plan using the **chg-dpl** MML command. Refer to the *Cisco Media Gateway Controller Software Release 7 Dial Plan Guide* for more information.
- If there are no logs that indicate that the dial plan was loaded incorrectly, then proceed to Step 2.
- Step 2** Contact the Cisco TAC to further analyze the problem and determine a solution. For more information about contacting the Cisco TAC, refer to the “Obtaining Technical Assistance” section on page xviii.
-

Bearer Channel Connection Problems

Bearer channels are the focus of everything that the Cisco MGC does. The main function of the Cisco MGC is to ensure that an ingress bearer channel at one endpoint can be successfully connected to an egress bearer channel at another endpoint.

The state of the bearer channels is often a good indicator of the overall health of the system. Procedures for determining the state of your bearer channels can be found in the “Verifying CIC States” section on page 3-13.

Troubleshooting Bearer Channel Connection Procedures

The following sections contains procedures that are related to resolving problems associated with the Cisco MGC node’s bearer channel connections:

- Setting the Administrative State, page 8-70
- Querying Local and Remote CIC States, page 8-76
- Performing CIC Validation Tests, page 8-78
- Resolving ISDN D-Channel Discrepancies, page 8-83
- Unblocking CICs, page 8-86
- Resetting CICs, page 8-87
- Resolving Stuck CICs, page 8-87
- Auditing Call States, page 8-91
- Stopping Calls, page 8-91
- Auditing an MGCP Media Gateway, page 8-94
- Running a Manual Continuity Test, page 8-96
- Verifying Continuity Test Settings, page 8-96
- Resolving an SRCP Audit Alarm, page 8-97
- Media Gateway IP Destination/Link Out-of-Service, page 8-98
- CIC Mismatch (One-Way Audio), page 8-99
- Calls Fail at the Cisco MGC, page 8-101
- Modifying Redundant Link Manager Timers, page 8-101

Setting the Administrative State

You can use the **set-admin-state** MML command to change the administrative state of various components. A platform info log is generated every time the **set-admin-state** MML command is entered. An alarm is generated every time the **set-admin-state** MML command is entered at either the Cisco MGC, media gateway, signaling service, or trunk group level.

The procedures that describe how to use this command are listed below:

- Setting the Administrative State of a Cisco MGC, page 8-71
- Setting the Administrative State of a Media Gateway, page 8-71
- Setting the Administrative State of a Trunk Group, page 8-72
- Setting the Administrative State of a Signaling Service, page 8-73
- Setting the Administrative State of Spans, page 8-73
- Setting the Administrative State of CICs, page 8-75

Setting the Administrative State of a Cisco MGC

To set the administrative state of a Cisco MGC, perform the following steps:

Step 1 Log in to the active Cisco MGC, start an MML session, and enter the following command:

```
set-admin-state:mgc:state
```

Where:

- *mgc*—The MML name of the desired Cisco MGC.
- *state*—The desired administrative state. The valid states are listed below:
 - *lock*—Makes all bearer channels unavailable for call processing. If the state is set to lock, active calls go into pending state, where calls remain up until either party voluntarily releases the call. New calls are disallowed.
 - *unlock*—Makes all bearer channels available for call processing. If the state is set to unlock, the Cisco MGC becomes available. New calls are allowed to use the unlocked bearer channels.
 - *reset*—Clears local and remote blocking on all bearer channels and they take on the blocking view of remote side.

For example, to set the administrative state of a Cisco MGC called *mgc1* to unlock, enter the following command:

```
set-admin-state:mgc1:unlock
```

Step 2 Verify that the state of the Cisco MGC has changed by entering the **rtrv-admin-state** MML command, as described in the “Retrieving the Administrative State of a Cisco MGC” section on page 3-59.

Setting the Administrative State of a Media Gateway

To set the administrative state of an associated media gateway, perform the following steps:

Step 1 Log in to the active Cisco MGC, start an MML session, and enter the following command:

```
set-admin-state:gway:state
```

Where:

- *gway*—The MML name of the desired media gateway.



Note

Not all media gateway types are applicable. Supported types are CU, MUX, MGW, and AVM external nodes.

- *state*—The desired administrative state. The valid states are listed below:
 - *lock* —Makes all bearer channels associated with the media gateway unavailable for call processing. If the state is set to lock, active calls on the affected bearer channels go into pending state, where calls remain up until either party voluntarily releases the call. New calls are disallowed on the affected bearer channels.
 - *unlock*—Makes all bearer channels associated with the media gateway available for call processing. If the state is set to unlock, the media gateway becomes available. New calls are allowed to use the affected bearer channels.

- **reset**—Clears local and remote blocking on the bearer channels associated with the media gateway and these bearer channels take on the blocking view of remote side.

For example, to set the administrative state of a media gateway called `sfgway` to lock, enter the following command:

```
set-admin-state:sfgway:lock
```

- Step 2** Verify that the state of the media gateway has changed by entering the **rtrv-admin-state** MML command, as described in the “Retrieving the Administrative State of a Media Gateway” section on page 3-60.

Setting the Administrative State of a Trunk Group

To set the administrative state of an trunk group, perform the following steps:

- Step 1** Log in to the active Cisco MGC, start an MML session, and enter the following command:

```
set-admin-state:trkgrp:state
```

Where:

- *trkgrp*—The MML name of the desired trunk group.



Note

This command can only be used for time-division multiplexing (TDM) trunk groups. Allow the corresponding MML name for component type "0020".

- *state*—The desired administrative state. The valid states are listed below:
 - **lock** —Makes all bearer channels associated with the trunk group unavailable for call processing. If the state is set to lock, active calls on the affected bearer channels go into pending state, where calls remain up until either party voluntarily releases the call. New calls are disallowed on the affected bearer channels.
 - **unlock**—Makes all bearer channels associated with the trunk group available for call processing. If the state is set to unlock, the media gateway becomes available. New calls are allowed to use the affected bearer channels.
 - **reset**—Clears local and remote blocking on the bearer channels associated with the trunk group and these bearer channels take on the blocking view of remote side.

For example, to set the administrative state of a trunk group called `trunkgrp1` to lock, enter the following command:

```
set-admin-state:trunkgrp1:lock
```

- Step 2** Verify that the state of the trunk group has changed by entering the **rtrv-admin-state** MML command, as described in the “Retrieving the Administrative State of a Trunk Group” section on page 3-60.

Setting the Administrative State of a Signaling Service

To set the administrative state of a signaling service, perform the following steps:

Step 1 Log in to the active Cisco MGC, start an MML session, and enter the following command:

```
set-admin-state:sig_srv:state
```

Where:

- *sig_srv*—The MML name of the desired signaling service. The following signaling service types are valid for this command:
 - For in-band TDM up to MUX and then time switched to TDM media and sent to the Cisco MGC.
 - For in-band TDM signaling up to CU and then encapsulated and sent over IP to the Cisco MGC.
 - For in-band TDM signaling up to the media gateway and then converted to NI2 and sent to the Cisco MGC over IP (that is, FE box<-sig/tdm->media gateway<-NI2/IP-> Cisco MGC).
 - Signaling service or routeset associated with a DPC.
 - EISUP signaling service.
- *state*—The desired administrative state. The valid states are listed below:
 - lock —Makes all bearer channels associated with the signaling service unavailable for call processing. If the state is set to lock, active calls on the affected bearer channels go into pending state, where calls remain up until either party voluntarily releases the call. New calls are disallowed on the affected bearer channels.
 - unlock—Makes all bearer channels associated with the signaling service available for call processing. If the state is set to unlock, the media gateway becomes available. New calls are allowed to use the affected bearer channels.

For example, to set the administrative state of a signaling service called nassrv1 to lock, enter the following command:

```
set-admin-state:nassrv1:lock
```

Step 2 Verify that the state of the Cisco MGC has changed by entering the **rtrv-admin-state** MML command, as described in the “Retrieving the Administrative State of a Signaling Service” section on page 3-60.

Setting the Administrative State of Spans

To set the administrative state of a single span, perform the following steps:

Step 1 Log in to the active Cisco MGC, start an MML session, and enter the following command:

```
set-admin-state:sig_srv:span=x:state
```

Where:

- *sig_srv* is the MML name of the signaling service. The following signaling service types are valid for this command:
 - For in-band TDM up to MUX and then time switched to TDM media and sent to the Cisco MGC.
 - For in-band TDM signaling up to CU and then encapsulated and sent over IP to the Cisco MGC.

- For in-band TDM signaling up to the media gateway and then converted to NI2 and sent to the Cisco MGC over IP (that is, FE box<-sig/tdm->media gateway<-NI2/IP-> Cisco MGC).
- Signaling service or routeset associated with a DPC.
- EISUP signaling service.
- *x*—A16-bit value that identifies an ISDN/PRI physical cable.
- *state*—The desired administrative state. The valid states are listed below:
 - *lock*—Makes all bearer channels associated with the span unavailable for call processing. If the state is set to lock, active calls on the affected bearer channels go into pending state, where calls remain up until either party voluntarily releases the call. New calls are disallowed on the affected bearer channels.
 - *unlock*—Makes all bearer channels associated with the span available for call processing. If the state is set to unlock, the span becomes available. New calls are allowed to use the affected bearer channels.

For example, to set the administrative state of span number 2 associated with a signaling service called *ss7svc1* to unlock, you would enter the following command:

```
set-admin-state:ss7svc1:span=2:lock
```

- Step 2** Verify that the state of the bearer channels have changed by entering the **rtrv-admin-state** MML command, as described in the “Retrieving the Administrative State of Spans” section on page 3-61.
-

To set the administrative state of a bearer channel or a range of bearer channels in a span, perform the following steps:

- Step 1** Log in to the active Cisco MGC, start an MML session, and enter the following command:

```
rtrv-admin-state:sig_srv:span=x,bc=y[,rng=range]:state
```

Where:

- *sig_srv* is the MML name of the signaling service. The following signaling service types are valid for this command:
 - For in-band TDM up to MUX and then time switched to TDM media and sent to the Cisco MGC.
 - For in-band TDM signaling up to CU and then encapsulated and sent over IP to the Cisco MGC.
 - For in-band TDM signaling up to the media gateway and then converted to NI2 and sent to the Cisco MGC over IP (that is, FE box<-sig/tdm->media gateway<-NI2/IP-> Cisco MGC).
 - Signaling service or routeset associated with a DPC.
 - EISUP signaling service.
- *x*—A16-bit value that identifies an ISDN/PRI physical cable.
- *y*—A numeric value that identifies the non-ISUP bearer channel number.
- *range*—A value such that *y+range* is a valid bearer channel number. The administrative state for all bearer channels between *y* and *y+range* are retrieved.
- *state*—The desired administrative state. The valid states are listed below:

- lock—Makes the specified bearer channels unavailable for call processing. If the state is set to lock, active calls on the affected bearer channels go into pending state, where calls remain up until either party voluntarily releases the call. New calls are disallowed on the affected bearer channels.
- unlock—Makes the specified bearer channels available for call processing. If the state is set to unlock, the bearer channels become available. New calls are allowed to use the affected bearer channels.

For example, to set the administrative state of bearer channels numbers 2 through 6, associated with a signaling service called `ss7svc1`, to unlock, you would enter the following command:

```
rtrv-admin-state:ss7svc1:span=2,bc=2,rng=5:unlock
```

- Step 2** Verify that the state of the bearer channels have changed by entering the **rtrv-admin-state** MML command, as described in the “Retrieving the Administrative State of Spans” section on page 3-61.

Setting the Administrative State of CICs

To set the administrative state of a CIC or a range of CICs, perform the following steps:

- Step 1** Log in to the active Cisco MGC, start an MML session, and enter the following command:

```
set-admin-state:sig_srv:cic=number[,rng=range]:state
```

Where:

- *sig_srv* is the MML name of the signaling service. The following signaling service types are valid for this command:
 - For in-band TDM up to MUX and then time switched to TDM media and sent to the Cisco MGC.
 - For in-band TDM signaling up to CU and then encapsulated and sent over IP to the Cisco MGC.
 - For in-band TDM signaling up to the media gateway and then converted to NI2 and sent to the Cisco MGC over IP (that is, FE box<-sig/tdm->media gateway<-NI2/IP-> Cisco MGC).
 - Signaling service or routeset associated with a DPC.
 - EISUP signaling service.
- *number*—A valid CIC number.
- *range*—A value such that *y+range* is a valid CIC number. The administrative state for all CICs between *y* and *y+range* are retrieved.
- *state*—The desired administrative state. The valid states are listed below:
 - lock—Makes all bearer channels associated with the CICs unavailable for call processing. If the state is set to lock, active calls on the affected bearer channels go into pending state, where calls remain up until either party voluntarily releases the call. New calls are disallowed on the affected bearer channels.
 - unlock—Makes all bearer channels associated with the CICs available for call processing. If the state is set to unlock, the CICs become available. New calls are allowed to use the affected bearer channels.
 - reset—Clears local and remote blocking on the bearer channels associated with the CICs and these bearer channels take on the blocking view of remote side.

For example, to set the administrative state of CICs 2 through 11, associated with a signaling service called `ss7svc1`, to lock, you would enter the following command:

```
set-admin-state:ss7svc1:cic=2, rng=9:lock
```

- Step 2** Verify that the state of the Cisco MGC has changed by entering the **rtrv-admin-state** MML command, as described in the “Retrieving the Administrative State of CICs” section on page 3-62.

Querying Local and Remote CIC States

In the course of troubleshooting problems with your bearer channels, you may need to query the local and remote states of the related CICs, to verify that they match. To query the local and remote states of a single CIC or a range of CICs, log in to the active Cisco MGC, start an MML session, and enter the following command:

```
query-cic:pt_code:cic=number[, rng=range]
```

Where:

- *pt_code*—The MML name for the point code associated with the affected CICs.
- *number*—The number of the first CIC in the range of affected CICs.
- *range*—A number such that *number+range* is the number of the last CIC in the range of affected CICs. All CICs between *number* and *number+range* are displayed.



Note

Not all SS7 variants support the querying of CICs. If this command is executed on a signaling service that is configured for an SS7 variant that does not support the querying of CICs, an error code, SABL, is returned once the query operation times out. Refer to the *Cisco Media Gateway Controller Software Release 7 MML Command Reference Guide* for more information on the SABL error code.



Note

The Cisco MGC software can be configured to issue individual or group supervision messages for point codes that are associated with an ISUP signaling service. ISUP signaling services issue group supervision messages by default. If an ISUP signaling service is configured to issue individual supervision messages, the *range* option cannot be used with this command. Querying of CICs associated with an ISUP signaling service configured to issue individual supervision messages can only be done one CIC number at a time.

For example, to query the state of CICs 20 through 24, associated with a point code called `dpc1`, you would enter the following command:

```
query-cic:dpc1:cic=20, rng=4
```

The system responds with a message similar to the following:

```
Media Gateway Controller - MGC-01 2000-01-12 15:19:51
M RTRV
"dpc1:CIC=20;LPST=IS;LSST=IDLE;RPST=IS;RSST=IDLE"
"dcp1:CIC=21;LPST=IS;LSST=IDLE;RPST=IS;RSST=IDLE"
"dpc1:CIC=22;LPST=IS;LSST=IDLE;RPST=IS;RSST=IDLE"
"dpc1:CIC=23;LPST=IS;LSST=IDLE;RPST=IS;RSST=IDLE"
"dpc1:CIC=24;LPST=OOS;LSST=IDLE_LOC_BLOC;RPST=IS;RSST=IDLE"
```

The response lists the local and remote primary and secondary states of the requested CICs. If the response indicates that the mismatch is due to a problem on the local side, you can attempt to resolve the state mismatch using the instructions in the “Resolving Local and Remote CIC State Mismatch” section on page 8-77. If the response indicates that the mismatch is due to a problem on the remote side, you must contact the personnel at the remote site to resolve the problem.

The valid values for the fields found in the response to this command are as follows:

- LPST and RPST—Local primary state and remote primary state
 - IS—In-Service
 - OOS—Out-of-Service
 - TRNS—Transient; the state is currently being changed
- LSST and RSST—Local secondary state and remote secondary state
 - N/A—Not available
 - UNEQUIPPED—Unequipped
 - IC_BUSY—Incoming is busy
 - IC_BUSY_LOC_BLOC—Incoming is busy, blocked locally
 - IC_BUSY_REM_BLOC—Incoming is busy, blocked remotely
 - IC_BUSY_BOTH_BLOC—Incoming is busy, blocked both remotely and locally
 - OG_BUSY—Outgoing is busy
 - OG_BUSY_LOC_BLOC—Outgoing is busy, blocked locally
 - OG_BUSY_REM_BLOC—Outgoing is busy, blocked remotely
 - OG_BUSY_BOTH_BLOC—Outgoing is busy, blocked both remotely and locally
 - IDLE—The circuit is idle, available for use
 - IDLE_LOC_BLOC—Idle, blocked locally
 - IDLE_REM_BLOC—Idle, blocked locally
 - IDLE_BOTH_BLOC—Idle, blocked both locally and remotely

Resolving Local and Remote CIC State Mismatch

When the local and remote states for CICs do not match and the problem lies with the local CIC states, you can attempt to resolve the mismatch using an MML command. To do this, log in to the active Cisco MGC, start an MML session, and enter the following command:

```
query-cic:pt_code:cic=number[,rng=range],rslv
```

Where:

- *pt_code*—The MML name for the point code associated with the affected CICs.
- *number*—The number of the first CIC in the range of affected CICs.
- *range*—A number such that *number+range* is the number of the last CIC in the range of affected CICs. The system attempts to resolve state mismatches for all CICs between *number* and *number+range*.

**Note**

The **rslv** option can only be used if your system used ANSI SS7 signaling. If your system uses ITU SS7 signaling and you use this command, the **rslv** option is ignored and a regular **query-cic** operation is performed.

**Note**

The Cisco MGC software can be configured to issue individual or group supervision messages for point codes that are associated with an ISUP signaling service. ISUP signaling services issue group supervision messages by default. If an ISUP signaling service is configured to issue individual supervision messages, the *range* option cannot be used with this command. Resolving of local and remote CIC state mismatch can only be done one CIC number at a time for point codes associated with an ISUP signaling service configured to issue individual supervision messages.

If the command fails in its attempt to resolve the local and remote CIC state mismatch, contact the Cisco TAC for assistance. Refer to the “Obtaining Technical Assistance” section on page xviii for more information about contacting the Cisco TAC.

Performing CIC Validation Tests

When performing initial turn-up of circuits or in troubleshooting certain problems with your bearer channels, you may want to perform a circuit validation test to verify that the properties defined in the Cisco MGC for the affected bearer channels match the associated properties defined in the far-end exchange.

**Note**

CIC validation tests can only be performed on CICs associated with ANSI SS7-based DPCs.

To perform a circuit validation test, complete the following steps:

Step 1

Start an MML session on the active Cisco MGC and validate the properties for a particular circuit identification code (CIC) using the following command:

```
vld-cic:dest_pc:cic=number
```

Where:

- *dest_pc*—The MML name for the DPC associated with the affected CIC.
- *number*—The trunk identification number for the affected CIC.

If the circuit validation test is passed, the system returns a message similar to the following:

```
Media Gateway Controller - MGC-01 2000-03-07 09:35:19
M RTRV
"dms100-pc:CIC=105, PASSED"
```

If the circuit validation test is failed, the system returns a message similar to the following:

```
Media Gateway Controller - MGC-01 2000-03-07 09:35:19
M RTRV
"dms100-pc:CIC=105, FAIL"
LOC: GRP=DIG, SEIZ=EVEN, ALM=UNK, COT=NONE
LOC: TRK=1003, A_CLLI=dms1003****, Z_CLLI=na*****
REM: GRP=DIG, SEIZ=ODD, ALM=SOFT, COT=STAT
```

The fields in the LOC line are values associated with the Cisco MGC. The fields in the REM line are values associated with the far-end exchange. The valid values for those fields are described below.

- GRP—Circuit group carrier indicator. The values in these fields should be the same in the LOC and REM lines. The valid values for this field are:
 - UNK—Unknown circuit group carrier type
 - ANL—Analog circuit group carrier type
 - DIG—Digital circuit group carrier type
 - AND—Analog and digital circuit group carrier type
- SIEZ—Double seizing indicator. The values for this field in the LOC line should be logically opposite to the value for the REM line. The valid values for this field are:
 - NONE—No circuit control. When one line is set to NONE, the other should be set to ALL.
 - ALL—All circuit control. When one line is set to ALL, the other should be set to NONE.
 - EVEN—Even circuit control. When one line is set to EVEN, the other should be set to ODD.
 - ODD—Odd circuit control. When one line is set to ODD, the other should be set to EVEN.
- ALM—Alarm carrier indicator. The values in these fields should be the same in the LOC and REM lines. The valid values for this field are:
 - UNK—Unknown alarm carrier
 - SOFT—Software alarm carrier
 - HARD—Hardware alarm carrier
- COT—Continuity check requirements indicator. The values in these fields should be the same in the LOC and REM lines. The valid values for this field are:
 - UNK—Unknown continuity check requirements
 - NONE—No continuity check requirements
 - STAT—Statistical continuity check requirements
 - PERC—Per call continuity check requirements
- TRK—Trunk number. This field is always displayed in the LOC line. It is only displayed in the REM line when the circuit identification names for the Cisco MGC and the far-end exchange do not match.
- A_CLLI—Common language location identifier (CLLI) code for either the far-end exchange or the Cisco MGC. The CLLIs for each are sorted alphabetically, and the A_CLLI field is populated with the CLLI that is found to be first. This field is always displayed in the LOC line. It is displayed in the REM line only when the CLLIs for the Cisco MGC and the far-end exchange do not match.
- Z_CLLI—CLLI code for either the far-end exchange or the Cisco MGC. The CLLIs for each are sorted alphabetically, and the Z_CLLI field is populated with the CLLI that is found to be second. This field is always displayed in the LOC line. It is displayed in the REM line only when the CLLIs for the Cisco MGC and the far-end exchange do not match.

If the circuit validation test passes, proceed to Step 14.

If the circuit validation test fails, proceed to Step 2.

- Step 2** Determine which settings are not correct by comparing the values displayed in the LOC field (from the Cisco MGC) to those in the REM field (from the associated far-end exchange), based on the field descriptions found above.
- Step 3** Consult your provisioning records to determine whether the settings on the Cisco MGC and/or the associated far-end exchange need to be modified to resolve the error.

If the settings on the Cisco MGC need to be modified to resolve the error, proceed to Step 4.

If the settings on the associated far-end exchange need to be modified to resolve the error, contact the provider that operates the switch and work with them to resolve the configuration error.

Step 4 Identify the signaling service associated with the affected DPC using the following command:

```
prov-rtrv:ss7path:"all"
```

The system returns a message similar to the following:

```
mgc-01 - Media Gateway Controller 2000-09-26 15:55:17
M RTRV
"session=active:ss7path"
/*
NAME          DPC          MDO          CUSTGRPID CUSTGRPTBL  SIDE
----          -
ss7am401a am401a-pc  ANSISS7_STANDARD 0000      0101      network
ss7am702b am702b-pc  ANSISS7_STANDARD 0000      0101      network
ss7inet1  inet sp1-pc  ANSISS7_STANDARD 0000      0101      network
ss7am408a am408a-pc  ANSISS7_STANDARD 0000      0101      network
ss7am408b am408b-pc  ANSISS7_STANDARD 0000      0101      network
ss7inet2  inet sp2-pc  ANSISS7_STANDARD 0000      0101      network
ss7dms    dms100-pc  ANSISS7_STANDARD 0000      0101      network
ss7am401b am401b-pc  ANSISS7_STANDARD 0000      0101      network
ss7am608b am608b-pc  ANSISS7_STANDARD 0000      0101      network
ss7sc2200 sc2200-pc  ANSISS7_STANDARD 0000      0101      network
```

The response lists the SS7 signaling services and their associated DPCs. Search for the DPC associated with the trunk to identify the name of the SS7 signaling service. In the example, **dms100-pc** is the name of the DPC associated with the trunk. The SS7 signaling service names are in the column to the immediate left of the DPCs, so the name of the associated SS7 signaling service in the example is **ss7dms**.

Step 5 Identify the MML names of the mismatched settings for the affected signaling service found in Step 4 using the following command:

```
prov-rtrv:sigsvccprop:name="sig_serv"
```

Where *sig_serv* is the MML name of the affected signaling service.

The system returns a message similar to the following:

```
MGC-01 - Media Gateway Controller 2000-09-26 15:57:29
M RTRV
"session=active:sigsvccprop"
/*
adjDestinations = 16
AlarmCarrier = 0
BOrigStartIndex = 0
BothwayWorking = 1
BTermStartIndex = 0
CctGrpCarrier = 2
CGBA2 = 0
CircHopCount = 0
CLIPess = 0
CotInTone = 2010
CotOutTone = 2010
CotPercentage = 0
dialogRange = 0
ExtCOT = Loop
ForwardCLIIinIAM = 1
ForwardSegmentedNEED = 1
GLARE = 0
GRA2 = 0
```

```

GRSEnabled = false
InternationalPrefix = 0
layerRetries = 2
layerTimer = 10
maxMessageLength = 250
mtp3Queue = 1024
NationalPrefix = 0
NatureOfAddrHandling = 0
Normalization = 0
OMaxDigits = 24
OMinDigits = 0
OOverlap = 0
OwnClli = na
RedirMax = 3
restartTimer = 10
RoutePref = 0
sendAfterRestart = 16
slsTimer = 300
srtTimer = 300
sstTimer = 300
standard = ANSI92
SwitchID = 0
TMaxDigits = 24
TMinDigits = 0
TOverlap = 0
variant = SS7-ANSI
VOIPPrefix = 0

```

The response above can be mapped to the response to the circuit validation test in Step 1, as listed below:

- CctGrpCarrier—The value in this field maps to the value in the GRP field, as follows:
 - 0—Equal to UNK (unknown carrier) in the GRP field.
 - 1—Equal to ANL (analog carrier) in the GRP field.
 - 2—Equal to DIG (digital carrier) in the GRP field.
 - 3—Equal to AND (analog and diglossia carrier) in the GRP field.
- Glare—The value in this field maps to the value in the SEIZ field, as follows:
 - 0 or 3—Equal to NONE (no circuit control) in the SEIZ field.
 - 1—Equal to ALL (all circuit control) in the SEIZ field.
 - 2—Equal to ODD (odd circuit control) in the SEIZ field when the OPC is less than the associated DPC. Equal to EVEN (even circuit control) in the SEIZ field when the OPC is greater than the associated DPC.
- AlarmCarrier—The value in this field maps to the value in the ALM field, as follows:
 - 0—Equal to UNK (unknown) in the ALM field.
 - 1—Equal to SOFT (software handling) in the ALM field.
 - 2—Equal to HARD (hardware handling) in the ALM field.
- CotPercentage and ExtCOT—The values in these field maps to the value in the COT field, as follows:
 - CotPercentage is undefined and ExtCOT is *not* set to *Loop* or *Transponder*—Equal to UNK (unknown continuity check requirements) in the COT field.
 - CotPercentage is set to any value and ExtCOT is *not* set to *Loop* or *Transponder*—Equal to NONE (no continuity check requirements) in the COT field.

- CotPercentage is greater than 0 and less than 100 and ExtCOT is set to *Loop* or *Transponder*—Equal to STAT (statistical continuity check requirements) in the COT field.
- CotPercentage is set to 100 and ExtCOT is set to *Loop* or *Transponder*—Equal to PERC (per call continuity check requirements) in the COT field.

Step 6 Start a provisioning session as described in the “Starting a Provisioning Session” section on page 3-63.

Step 7 Modify the appropriate signaling service settings using the following command:

```
prov-ed:sigsvccprop:name="sig_svc",param_name="param_value",param_name="param_value",...
```

Where:

- *sig_svc*—The MML name for the affected signaling service.
- *param_name*—The MML name for a mismatched setting.
- *param_value*—The correct value for a mismatched setting.

For example, to change the settings for the COT to per call and seizing (glare) to no circuit control for the ss7dms signaling service, you would enter the following command:

```
prov-ed:sigsvccprop:name="ss7dms",ExtCOT="Loop", CotPercentage="100",GLARE="0"
```

Step 8 If your Cisco MGC is provisioned for a switched environment and you need to modify the COT and/or seizing (glare) properties, the trunk group properties need to be modified.

If you need to modify the trunk group properties, proceed to Step 9.

If you do not need to modify the trunk group properties, proceed to Step 12.

Step 9 Identify the trunk group associated with the affected DPC using the following command:

```
prov-rtrv:trnkgrp:svc="sig_serv"
```

Where: *sig_serv*—The MML name of the SS7 signaling service identified in Step 4.

The system returns a message similar to the following:

```
MGC-01 - Media Gateway Controller 2000-09-26 15:55:17
M RTRV
"session=active:trnkgrp"
/*
NAME    CLLI          SVC      TYPE          SELSEQ        QABLE
----    -
1003    DMS100CLLIss7dms  TDM_ISUP      ASC           N
```

The response lists the trunk group associated with the affected SS7 signaling service. The MML name of the trunk group is found in the NAME column. In the example, **ss7dms** is the name of the SS7 signaling service associated with the trunk. The trunk group names are in the first column, so the name of the associated trunk group in the example is **1003**.

Step 10 Identify the MML names of the mismatched settings for the affected trunk group found in Step 9 using the following command:

```
prov-rtrv:trnkgrpprop:name="trnk_grp"
```

Where: *trnk_grp*—The MML name of the affected trunk group.

The system returns a message similar to the following:

```
mgc-01 - Media Gateway Controller 2000-09-26 15:57:29
M RTRV
"session=active:trnkgrpprop"
/*
BOrigStartIndex = 1
BTermStartIndex = 2
```



```

CarrierIdentity = 0333
CLLI = GR31764KB5
CompressionType = 1
CotPercentage = 1
CustGrpId = V123
EchoCanRequired = 0
ExtCOT = Loop
GLARE = 2
Npa = 919
RingNoAnswer = 100000
SatelliteInd = 0
ScreenFailAction = 0
*/

```

Step 11 Modify the appropriate trunk group settings using the following command:

```
prov-ed:trnkgrp:name="trnk_grp",param_name="param_value",param_name="param_value",...
```

Where:

- *trnk_grp*—The MML name for the affected trunk group.
- *param_name*—The MML name for a mismatched setting.
- *param_value*—The correct value for a mismatched setting.



Note The values for the COT and/or seizing properties entered here should match the values set in Step 7.

For example, to change the settings for the COT to per call and seizing (glare) to no circuit control for the trnkgrpds trunk group, you would enter the following command:

```
prov-ed:ztrnkgrp:name="trnkgrpds",ExtCOT="Loop", CotPercentage="100",GLARE="0"
```

Step 12 Activate your new configuration as described in the “Saving and Activating your Provisioning Changes” section on page 3-64.

Step 13 Return to Step 1 and enter the **vld-cic** command again.

If the response indicates that the test has passed, proceed to Step 14.

If the response indicates that the test has failed, resume performing this procedure from Step 2 and modify the mismatched settings identified in the latest command response.

Step 14 Repeat Steps 1 through 13 for each additional CIC you want to test.

Resolving ISDN D-Channel Discrepancies

When there is a mismatch between the D-channels configured on the Cisco MGC and those configured on the associated media gateway, an ISDN log message is generated. To resolve the log message, complete the following steps:

Step 1 Enter the following command at the active Cisco MGC to change directories:

```
cd $BASEDIR/etc
```

Step 2 Determine the component IDs associated with the D-channel number identified in the log text by searching for the D-channel number in the data files.

For example, if the log message contains the following text:

```
PROT_ERR_ISDN:Error message from ISDN:Receive MGMT_ERROR_IND for set 1, channel 2854
```

The D-channel number in the example is **2854**. Therefore, you would search for occurrences of D-channel **2854** in the data files.

Enter the following command to search the data files for the identified D-channel number:

```
grep d_num *.dat
```

Where *d_num* is the D-channel number identified in the alarm message.

The system returns a message similar to the following:

```
sigChanDev.dat:001002bd 00160002 1 0034015e 00030011 00060001 2854
sigChanDev.dat:001002be 00160002 1 0034015e 00030011 00060002 2854
```

The response lists the data file(s) in which the D-channel number found, along with the associated properties. In the example above, the D-channel number, **2854**, is found twice in the **sigChanDev.dat** file. The component IDs are in the column immediately following the data file name. So, in this example, the component IDs are **001002bd** and **001002be**.

- Step 3** Determine the MML name of an IP link associated with one of the component IDs you identified in Step 2 using the following command:

```
grep comp_ID components.dat
```

Where: *comp_ID* — A component ID identified in Step 2.

The system returns a message similar to the following:

```
001002bd 0034015e "bh531-31" "IP link-backhaul svc mgx8260 EAST"
```

The response lists the properties associated with your selected component ID. The MML name for the IP link is in the third column in the response. In the above example, "**bh531-31**" is the MML name for the IP link.

- Step 4** Repeat Step 3 for each component ID identified in Step 2.

- Step 5** Start an MML session from the active Cisco MGC and enter the following command to determine the MML name for the signaling service associated with the IP link(s) identified in Step 3:

```
prov-rtrv:iplnk:name="ip_link"
```

Where: *ip_link* — The MML name for an IP link(s) identified in Step 3.

The system returns a message similar to the following:

```
Media Gateway Controller 2000-06-08 13:49:53
M RTRV
  "session=active:iplnk"
/*
NAME = bh531-31
DESC = IP link-backhaul svc mgx8260 EAST
SVC = bh531-3
IF = enif1
IPADDR = IP_Addr1
PORT = 7007
PEERADDR = 10.15.26.20
PEERPORT = 7007
PRI = 1
SIGSLOT = 11
SIGPORT = 38
*/
```

The response lists the properties associated with your selected IP link. The MML name for the signaling service associated with the link is in the SVC field. In the above example, **bh531-3** is the MML name for the signaling service. Note the values in the SIGSLOT and SIGPORT fields. These values are used later to determine whether the D-channel is defined on the media gateway.

- Step 6** Enter the following command to retrieve the properties for the signaling service identified in Step 5:

```
rtrv-dest:sig_serv
```

Where *sig_serv* is the MML name for a signaling service identified in Step 5.

The system returns a message similar to the following:

```
Media Gateway Controller 2000-06-08 13:50:26
M   RTRV
    "bh531-3:PKG=ISDNPRI,ASSOC=SWITCHED,PST=OOS,SST=UND"
```

- Step 7** Log into the associated media gateway and determine whether the D-channel is defined. Refer to the documentation for the media gateway for information on how to verify whether the D-channel is defined.

For example, to determine whether a D-channel is defined for a Cisco MGX8260 media gateway, you would enter the following command:

```
lsdchan 12.39
```

The values, **12.39**, specify the D-channel. These numbers are determined by adding 1 to the SIGSLOT and SIGPORT values identified in Step 5.

The media gateway responds with a message that indicates whether the D-channel is defined.

- Step 8** Consult your provisioning records and determine whether the identified D-channel should exist.

If your provisioning records indicate that the D-channel should exist, proceed to Step 9.

If your provisioning records indicate that the D-channel should *not* exist, proceed to Step 10.

- Step 9** Define the D-channel on the associated media gateway. Refer to the documentation for the media gateway for information on how to define a D-channel.

The procedure is finished.

- Step 10** Start a provisioning session as described in the “Starting a Provisioning Session” section on page 3-63.

- Step 11** Delete the appropriate D-channel(s) using the following command:

```
prov-dlt:iplnk:name="ip_link",...
```

Where *ip_link* is the MML name(s) for an IP link identified in Step 3.

For example, to delete a D-channel named bh531-31, you would enter the following command:

```
prov-dlt:iplink:name="bh531-31"
```

- Step 12** Delete the signaling service associated with the D-channel(s) using the following command:

```
prov-dlt:ipfaspath:name="sig_serv"
```

Where *sig_serv* is the MML name for a signaling service identified in Step 5.

For example, to delete a signaling service named bh531-3, you would enter the following command:

```
prov-dlt:ipfaspath:name="bh531-3"
```

- Step 13** Activate your new configuration as described in the “Saving and Activating your Provisioning Changes” section on page 3-64.

Unblocking CICs

You may need to unblock a CIC or a range of CICs on your Cisco MGC. There are two types of blocking on a CIC, local and remote.

Unblocking Locally Blocked CICs

To unblock a single CIC, log in to your active Cisco MGC, start an MML session and enter the following command:

```
unblk-cic:dest_pc:CIC=number
```

Where:

- *dest_pc*—The MML name of the DPC associated with the CICs to be unblocked.
- *number*—The number of the affected CIC.

For example, to unblock CIC number 2, which is associated with a DPC called dpc1, you would enter the following command:

```
unblk-cic:dpc1:CIC=2
```

To unblock a range of CICs, log in to your active Cisco MGC, start an MML session, and enter the following command:

```
unblk-cic:dest_pc:CIC=number,RNG=range
```

Where:

- *point_code*—The MML name of a DPC associated with the CICs you want to unblock.
- *number*—The number of the first CIC in the range of CICs you want to unblock.
- *range*—Specifies the end of the range of CICs to be unblocked.



Note

The Cisco MGC software can be configured to issue individual or group supervision messages for point codes that are associated with an ISUP signaling service. ISUP signaling services issue group supervision messages by default. If an ISUP signaling service is configured to issue individual supervision messages, the *range* option cannot be used with this command. Unblocking of CICs can only be done one CIC number at a time for point codes associated with an ISUP signaling service configured to issue individual supervision messages.

For example, to unblock CIC number 1 through 20, which are associated with a DPC called dpc1, you would enter the following command:

```
unblk-cic:dpc1:cic=1, rng=20
```

To verify that the CIC(s) have been successfully unblocked, retrieve the status of the affected CICs as described in the “Verifying CIC States” section on page 3-13. If the CIC(s) are still blocked, proceed to the “Resetting CICs” section on page 8-87.

Unblocking Remotely Blocked CICs

Generally, you cannot unblock a CIC that has been blocked remotely, because the block was set on the far-end. However, in some instances, a remotely blocked CIC is misreported, and you can fix this by resetting the CIC as described in the “Resetting CICs” section on page 8-87.

Resetting CICs

When trying to clear a blocked CIC or range of CICs, you may need to perform a reset on the affected CIC(s). To reset a single CIC, log in to your active Cisco MGC, start an MML session and enter the following command:

```
reset-cic:dest_pc:CIC=number
```

Where:

- *dest_pc*—The MML name of the DPC associated with the CICs to be reset.
- *number*—The number of the affected CIC.

For example, to reset CIC number 2, which is associated with a DPC called dpc1, you would enter the following command:

```
reset-cic:dpc1:CIC=2
```

To reset a range of CICs, log in to your active Cisco MGC, start an MML session, and enter the following command:

```
reset-cic:dest_pc:CIC=number,RNG=range
```

Where:

- *point_code*—The MML name of a DPC associated with the CICs you want to reset.
- *number*—The number of the first CIC in the range of CICs you want to reset.
- *range*—Specifies the end of the range of CICs to be reset.



Note

The Cisco MGC software can be configured to issue individual or group supervision messages for point codes that are associated with an ISUP signaling service. ISUP signaling services issue group supervision messages by default. If an ISUP signaling service is configured to issue individual supervision messages, the *range* option cannot be used with this command. Resetting of CICs can only be done one CIC number at a time for point codes associated with an ISUP signaling service configured to issue individual supervision messages.

For example, to reset CICs number 1 through 20, which are associated with a DPC called dpc1, you would enter the following command:

```
reset-cic:dpc1:cic=1, rng=20
```

To verify that the CIC(s) have been successfully reset, retrieve the status of the affected CICs as described in the “Verifying CIC States” section on page 3-13. If the CIC(s) are still blocked, proceed to the “Resolving Stuck CICs” section on page 8-87.

Resolving Stuck CICs

A stuck or hung CIC is a condition that occurs when one or more bearer channels associated with a single call instance refuses to return to the idle call state, despite attempts to manually clear it down using the **reset-cic** MML command. Stuck CICs are generally caused when transient network glitches or configuration errors trigger protocol state machine errors. Typically these conditions result in a mismatch between the CIC’s call state on the Cisco MGC and the call state for the associated span and bearer channel (also known as timeslot) on the media gateway.

The Cisco MGC is capable of automatically detecting and terminating stuck CICs. Refer to the *Release Notes for the Cisco Media Gateway Controller Software* for more information. With the addition of this functionality, the system runs an audit cron job once a day that verifies, using the **sta-aud** MML command, that the call states for the CICs on the Cisco MGC match the associated states for the spans and bearer channels on the media gateway. If the audit finds that the Cisco MGC call states on a CIC show that a call is in progress while the associated media gateway span and bearer channel states are idle, the system attempts to release the identified CIC using the **stp-call** MML command. The **stp-call** MML command monitors for the release of the CIC. If the CIC is not released within 1 to 2 minutes, the CIC is forcefully released. When a CIC is forcefully released, a minimal CDR is written, with a cause of Temporary Failure.

**Note**

If you suspect that you have stuck CICs, and you do not want to wait for the audit cron job to be performed, or if the audit cron job appears to be unable to clear your stuck CICs, perform the steps identified in the “Manually Resolving Stuck CICs” section on page 8-88.

**Note**

The format of the CDR is dependent upon how you have configured the associated XECfgParm.dat configuration parameters. For more information on XECfgParm.dat configuration, refer to the *Cisco Media Gateway Controller Software Release 7 Installation and Configuration Guide*. For more information on CDRs, refer to the *Cisco Media Gateway Controller Software Release 7 Billing Interface Guide*.

If you want to run the audit cron job more than once a day, increase the frequency of the audit in the mgcusr crontab entry. You must have system administration authority to use crontab. For more information on crontab, enter the UNIX command, **man crontab**, on your Cisco MGC.

**Note**

The audit cron job will not be run by the system if the call engine’s CPU load is greater than the limit set in the XECfgParm.dat file. For more information on XECfgParm.dat configuration, refer to the *Cisco Media Gateway Controller Software Release 7 Installation and Configuration Guide*.

If you are running a release prior to Release 7.4(11), you must contact the Cisco TAC for assistance in clearing stuck CICs. Refer to the “Obtaining Technical Assistance” section on page xviii for more information about contacting the Cisco TAC.

Manually Resolving Stuck CICs

If you want to manually resolve stuck CICs, perform the follow steps:

-
- Step 1** Set the logging level of the call engine process (eng-01) to *info*, using the procedure described in the “Changing the Log Level for Processes” section on page 8-6.
 - Step 2** Perform a call state audit, using the procedure described in the “Auditing Call States” section on page 8-91.

When you search the active system log file, look for a CP_INFO_CHAN_STATE message containing the following text:

```
NAS is idle, SC is busy
```

An example of this log message appears below:

```
Fri May 25 13:27:45:384 2001 | engine (PID 14217) <Info>
CP_INFO_CHAN_STATE:Mismatch in channel state, NAS is idle, SC is busy, span 0, channel 2
```

If you find this kind of CP_INFO_CHAN_STATE message in the active system log file, proceed to Step 3. Otherwise, contact the Cisco TAC for assistance. Refer to the “Obtaining Technical Assistance” section on page xviii for more information about contacting the Cisco TAC.

- Step 3** There should be two associated CP_ERR_AUEP messages, one containing information on the affected span and bearer channel and another containing information on the affected CIC. Search the active system log file for a CP_ERR_AUEP message containing the following text:

```
Audit:failed to audit end point
```

An example of these messages appears below:

```
Fri May 25 13:27:45:384 2001 | engine (PID 14217) <Error>
CP_ERR_AUEP:Audit:failed to audit end point nassvc1[00140001]/0/2
```

```
Fri May 25 13:27:45:384 2001 | engine (PID 14217) <Error>
CP_ERR_AUEP:Audit:failed to audit end point dpc1[00130002]/ffff/2
```

In the first message, which contains information on the affected span and bearer channel, the text that immediately follows the word “point” identifies the following:

- The MML name of the media gateway destination associated with the affected span and bearer channel (nassvc1 in the example).
- The internal hexadecimal code associated with the identified media gateway destination (00140001 in the example). This number appears in brackets.
- The affected span number, in hexadecimal (0 in the example).
- The affected bearer channel number, in hexadecimal (2 in the example).

In the second message, which contains information on the affected CIC, the text that immediately follows the word “point” identifies the following:

- The MML name of the DPC associated with the affected CIC (dpc1 in the example).
- The internal hexadecimal code associated with the identified DPC (00130002 in the example). This number appears in brackets.
- The affected span number, in hexadecimal (ffff in the example). This field for this type of message is always set to “ffff”, because there is no correlation to span in SS7 networks.
- The affected CIC number, in hexadecimal (2 in the example).

- Step 4** Convert the hexadecimal values for the span, bearer channel, and CIC into decimal values.
- Step 5** Using the information gathered in steps 3 and 4, stop the call on an affected CIC for its associated DPC, using the procedure described in the “Stopping Calls on CICs” section on page 8-94.
- Step 6** Using the information gathered in steps 3 and 4, stop the call on an affected span and bearer channel for its associated media gateway destination, using the procedure described in the “Stopping Calls on Spans” section on page 8-93.
- Step 7** Reset the affected CIC using the procedure in the “Resetting CICs” section on page 8-87.
- Step 8** Repeat steps 2 through 7, searching for additional sets of affected CICs, spans, and bearer channels, until you have addressed all of the stuck CICs identified by the call state audit.
- Step 9** Repeat steps 2 and 3, performing a second call state audit and searching the active system log file to determine whether the previously identified CICs are still stuck.

If the previously identified CICs are still stuck, proceed to Step 10. Otherwise, proceed to Step 13.

- Step 10** Forcefully end the call on the DPC and CICs identified in Step 3 by entering the following command:

```
kill-call:dest_pc:cic=num,confirm
```

**Caution**

The **kill-call** MML command forcibly ends calls locally. It does not send SS7 messages to the far-end. **Kill-call** should only be used when you are attempting to clear stuck CICs that cannot be cleared using the **stp-call** or **reset-cic** MML commands.

Where:

- *dest_pc*—MML name of the DPC identified in Step 3.
- *num*—Number of the stuck CIC identified in Step 3.

For example, to forcefully stop a call on CIC 215, which is associated with a DPC called *dpc1*, you would enter the following command:

```
kill-call:dpc1:cic=215,confirm
```

Repeat this step for each CIC you have identified as being stuck.

- Step 11** Forcefully end the call on the signaling service, spans, and bearer channels identified in Step 3 by entering the following command:

```
kill-call:sig_srv:span=span_num,bc=bear_chan,confirm
```

**Caution**

The **kill-call** MML command forcibly ends calls locally. It does not send SS7 messages to the far-end. **Kill-call** should only be used when you are attempting to clear stuck CICs that cannot be cleared using the **stp-call** or **reset-cic** MML commands.

Where:

- *sig_srv*—MML name of the signaling service identified in Step 3.
- *span_num*—Number of the span identified in Step 3.
- *bear_chan*—Number of the stuck bearer channel identified in Step 3.

For example, to forcefully stop a call on bearer channel 2, which is on span 2, and is associated with a signaling service called *nassvc1*, you would enter the following command:

```
kill-call:nassvc1:span=2,bc=2,confirm
```

Repeat this step for each bearer channel you have identified as being stuck.

- Step 12** Repeat steps 2 and 3, performing a third call state audit and searching the active system log file to determine whether the previously identified CICs are still stuck.

If the previously identified CICs are no longer stuck, proceed to Step 13. If these CICs are still stuck, perform a call trace as described in “Performing a Call Trace” section on page 8-102, and contact the Cisco TAC for assistance. Refer to the “Obtaining Technical Assistance” section on page xviii for more information about contacting the Cisco TAC.

- Step 13** Set the logging level of the call engine (eng-01) to *err*, using the procedure described in the “Changing the Log Level for Processes” section on page 8-6.

Auditing Call States

To run a call state audit, which compares the call states of the CICs on the Cisco MGC with the associated states of the spans and bearer channels on the media gateway, perform the following steps:

Step 1 Log in to the active Cisco MGC, start an MML session, and enter the following command:

```
sta-aud
```



Note The Cisco MGC does not indicate when the **sta-aud** MML command has completed its call state audit process. Wait a few minutes before proceeding to the next step.

The results of the call state audit are sent to the active system log file.

Step 2 View the active system log file as described in the “Viewing System Logs” section on page 8-4. If you see any call state mismatch logs in the active system log file, contact the Cisco TAC for assistance in resolving the call state mismatch. Refer to the “Obtaining Technical Assistance” section on page xviii for more information about contacting the Cisco TAC.

Step 3 Once you have finished audit the call states, enter the following command:

```
stp-aud
```

Stopping Calls

You can use the **stp-call** MML command to stop calls gracefully on all traffic channels associated with a specified system resource. The **stp-call** MML command is described in the following sections:



Note The **stp-call** MML command forcefully stops calls if a calls do not gracefully stop within two minutes of the execution of the command. Refer to the *Release Notes for the Cisco Media Gateway Controller Software* for more information.

- Stopping Calls on a Cisco MGC, page 8-91
- Stopping Calls on a Media Gateway, page 8-92
- Stopping Calls on a Trunk Group, page 8-92
- Stopping Calls on a Signaling Service, page 8-92
- Stopping Calls on Spans, page 8-93
- Stopping Calls on CICs, page 8-94

Stopping Calls on a Cisco MGC

To stop all active calls on all traffic channels on a Cisco MGC, log in to the active Cisco MGC, start an MML session, and enter the following command:

```
stp-call:mgc,confirm
```

Where *mgc* is the MML name of the desired Cisco MGC.

For example, to stop all active calls on all traffic channels on a Cisco MGC called `mgc1`, enter the following command:

```
stp-call:mgc1,confirm
```

Stopping Calls on a Media Gateway

To stop all active calls on all traffic channels on a media gateway, log in to the active Cisco MGC, start an MML session, and enter the following command:

```
stp-call:gway,confirm
```

Where *gway* is the MML name of the desired media gateway.



Note

Not all media gateway types are applicable. Supported types are CU, MUX, MGW, and AVM external nodes.

For example, to stop all active calls on all traffic channels on a media gateway called `sfgway`, enter the following command:

```
stp-call:sfgway
```

Stopping Calls on a Trunk Group

To stop all active calls on all traffic channels associated with a trunk group, log in to the active Cisco MGC, start an MML session, and enter the following command:

```
stp-call:trkgrp,confirm
```

Where *trkgrp* is the MML name of the desired trunk group.



Note

This command can only be used for TDM trunk groups. Allow the corresponding MML name for component type "0020".

For example, to stop all active calls on all traffic channels associated with a trunk group called `trunkgrp1`, enter the following command:

```
stp-call:trunkgrp1,confirm
```

Stopping Calls on a Signaling Service

To stop all active calls on all traffic channels associated with a signaling service, log in to the active Cisco MGC, start an MML session, and enter the following command:

```
stp-call:sig_srv,confirm
```

Where *sig_srv* is the MML name of the desired signaling service. The following signaling service types are valid for this command:

- For in-band TDM up to MUX and then time switched to TDM media and sent to the Cisco MGC.
- For in-band TDM signaling up to CU and then encapsulated and sent over IP to the Cisco MGC.
- For in-band TDM signaling up to the media gateway and then converted to NI2 and sent to the Cisco MGC over IP (that is, FE box<-sig/tdm->media gateway<-NI2/IP-> Cisco MGC).
- Signaling service or routeset associated with a DPC.

- EISUP signaling service.

For example, to stop all active calls on all traffic channels associated with a signaling service called `nassrv1`, enter the following command:

```
stp-call:nassrv1,confirm
```

Stopping Calls on Spans

To stop all active calls on all bearer channels associated with a single span, log in to the active Cisco MGC, start an MML session, and enter the following command:

```
stp-call:sig_srv:span=x,confirm
```

Where:

- *sig_srv* is the MML name of the signaling service. The following signaling service types are valid for this command:
 - For in-band TDM up to MUX and then time switched to TDM media and sent to the Cisco MGC.
 - For in-band TDM signaling up to CU and then encapsulated and sent over IP to the Cisco MGC.
 - For in-band TDM signaling up to the media gateway and then converted to NI2 and sent to the Cisco MGC over IP (that is, FE box<-sig/tdm->media gateway<-NI2/IP-> Cisco MGC).
 - Signaling service or routeset associated with a DPC.
 - EISUP signaling service.
- *x*—A16-bit value that identifies an ISDN/PRI physical cable.

For example, to stop all active calls on all bearer channels on a signaling service called `ss7svc1` associated with span number 1, enter the following command:

```
stp-call:ss7svc1:span=1,confirm
```

To stop all active calls on a bearer channel, or a range of bearer channels, for a span associated with a signaling service, log in to the active Cisco MGC, start an MML session, and enter the following command:

```
stp-call:sig_srv:span=x,bc=y[,rng=range],confirm
```

Where:

- *sig_srv* is the MML name of the signaling service. The following signaling service types are valid for this command:
 - For in-band TDM up to MUX and then time switched to TDM media and sent to the Cisco MGC.
 - For in-band TDM signaling up to CU and then encapsulated and sent over IP to the Cisco MGC.
 - For in-band TDM signaling up to the media gateway and then converted to NI2 and sent to the Cisco MGC over IP (that is, FE box<-sig/tdm->media gateway<-NI2/IP-> Cisco MGC).
 - Signaling service or routeset associated with a DPC.
 - EISUP signaling service.
- *x*—A16-bit value that identifies an ISDN/PRI physical cable.
- *y*—A numeric value that identifies the non-ISUP bearer channel number.
- *range*—A value such that *y+range* is a valid bearer channel number. The administrative state for all bearer channels between *y* and *y+range* are retrieved.

For example, to stop all active calls on all bearer channel numbers 2 through 6, associated with a signaling service called `ss7svc1`, enter the following command:

```
stp-call:ss7svc1:span=2,bc=2,rng=5,confirm
```

Stopping Calls on CICs

To stop all active calls on a CIC, or a range of CICs, associated with a signaling service, log in to the active Cisco MGC, start an MML session, and enter the following command:

```
stp-call:sig_srv:cic=number[,rng=range],confirm
```

Where:

- *sig_srv* is the MML name of the signaling service. The following signaling service types are valid for this command:
 - For in-band TDM up to MUX and then time switched to TDM media and sent to the Cisco MGC.
 - For in-band TDM signaling up to CU and then encapsulated and sent over IP to the Cisco MGC.
 - For in-band TDM signaling up to the media gateway and then converted to NI2 and sent to the Cisco MGC over IP (that is, FE box<-sig/tdm->media gateway<-NI2/IP-> Cisco MGC).
 - Signaling service or routeset associated with a DPC.
 - EISUP signaling service.
- *number*—A valid CIC number.
- *range*—A value such that *y+range* is a valid bearer channel number. The administrative state for all bearer channels between *y* and *y+range* are retrieved.

For example, to stop all active calls on CICs 2 through 11, associated with a signaling service called `ss7svc1`, enter the following command:

```
stp-call:ss7svc1:cic=2,rng=9,confirm
```

Auditing an MGCP Media Gateway

You can audit an MGCP media gateway from the Cisco MGC. The procedure to audit an MGCP media gateway is described in the following sections:

- Starting an MGCP Media Gateway Audit, page 8-94
- Retrieving an MGCP Media Gateway Audit, page 8-95

Starting an MGCP Media Gateway Audit

You can run an audit on a single MGCP media gateway, or on all of your provisioned MGCP media gateways. The Cisco MGC does not prompt you to indicate when the audit is complete. Please wait a few moments before retrieving the audit results as described in the “Retrieving an MGCP Media Gateway Audit” section on page 8-95.

To run an audit on a single MGCP media gateway, log on to the active Cisco MGC, start an MML session, and enter the following command:

```
sta-aud-gw:MGCP_sig_srv
```

Where *MGCP_sig_srv* is the MML name of the MGCP signaling service associated with the MGCP media gateway.

For example, to start an audit on an MGCP media gateway associated with an MGCP signaling service called T-1-16, you would enter the following command:

```
sta-aud-gw:T-1-16
```

To run an audit all of your MGCP media gateways, log on to the active Cisco MGC, start an MML session, and enter the following command:

```
sta-aud-gw:all
```

Retrieving an MGCP Media Gateway Audit

You can retrieve an audit for a single MGCP media gateway, or for audits on all of your MGCP media gateways. To retrieve an audit for a single MGCP media gateway, log on to the active Cisco MGC, start an MML session, and enter the following command:

```
rtrv-aud-gw:MGCP_sig_srv
```

Where *MGCP_sig_srv* is the MML name of the MGCP signaling service associated with the MGCP media gateway.

For example, to retrieve an audit on an MGCP media gateway associated with an MGCP signaling service called T-1-16, you would enter the following command:

```
rtrv-aud-gw:T-1-16
```

The system returns a response similar to the following:

```
Media Gateway Controller - MGC-01 2000-01-12 15:19:51
M COMPLD
  "SP1-MGCP1:Audit gw received at 2000-01-12 15:19:51
Audit GW PASSED
pass pn
pass pt - not alarmed
pass sl - not alarmed
pass nl
pass bp
pass cp
pass rp
pass nb
pass uc
pass ic
pass us
pass is"
```

The response indicates whether the audit has passed or failed. If the audit has failed, refer to the documentation for the associated MGCP media gateway for more information on troubleshooting the identified problem.

To retrieve audits run on all of your MGCP media gateways, log on to the active Cisco MGC, start an MML session, and enter the following command:

```
rtrv-aud-gw:all
```

The system returns a response similar to the one shown above, with a set of data for every MGCP media gateway associated with your system.

Running a Manual Continuity Test

To run a manual continuity test (COT) on a specified remote switch CIC, log in to the active Cisco MGC, start an MML session, and enter the following command:

```
tst-cot:pt_code:cic=number
```

Where:

- *pt_code*—The MML name of the point code associated with the CIC to be tested.
- *number*—The identification number of the CIC to be tested.

For example, to run a manual COT on CIC number 5 of a DPC named dpc1, you would enter the following command:

```
tst-cot:dpc1:cic=5
```

If the manual COT test should fail, verify the COT settings for the Cisco MGC and the associated media gateway, as described in the “Verifying Continuity Test Settings” section on page 8-96.

Verifying Continuity Test Settings

- Step 1** Verify that the COT properties for the associated SS7 signaling service or trunk group are correct by logging in to the active Cisco MGC, starting an MML session, and entering the following command:

```
prov-rtrv:component:name="comp_name"
```

Where:

- *component*—MML component type name for the SS7 signaling service or trunk group properties. Enter one of the following:
 - sigsvccprop—Component type for SS7 signaling service properties.
 - trnkgrpprop—Component type for trunk group properties.
- *comp_name*—MML name for the affected SS7 signaling service or trunk group.

For example, if you wanted to verify the properties for an SS7 signaling service called **ss7svc1**, you would enter the following command:

```
prov-rtrv:sigsvccprop:name="ss7svc1"
```

If your system has been properly configured for dial plan use, the system returns a response similar to the following:

```
MGC-01 - Media Gateway Controller 2001-06-01 10:09:47
M  RTRV
    "session=active:sigsvccprop"
    /*
adjDestinations = 16
AlarmCarrier = 0
BOrigStartIndex = 0
BothwayWorking = 1
BTermStartIndex = 1
CctGrpCarrier = 2
CGBA2 = 0
CircHopCount = 0
CLIPess = 0
CotInTone = 2010
```

```

CotOutTone = 2010
CotPercentage = 0
CustGrpId=2222
dialogRange = 0
ExtCOT = Loop
ForwardCLInIAM = 1
ForwardSegmentedNEED = 1
.
.
.

```

- Step 2** If your settings for the highlighted properties match what is displayed above, proceed to Step 5. Otherwise, you must modify the COT settings on your Cisco MGC. To begin modifying the COT settings, start a provisioning session as described in the “Starting a Provisioning Session” section on page 3-63.
- Step 3** Enter the following command to modify the COT settings on your Cisco MGC:
- ```
prov-ed:component:name="comp_name",cot_prop=value,cot_prop=value,...
```
- Where:
- *component*—MML component type name for the SS7 signaling service or trunk group properties. Enter one of the following:
    - *ss7path*—Component type for SS7 signaling services.
    - *trnkgrp*—Component type for trunk groups.
  - *comp\_name*—MML name for the affected SS7 signaling service or trunk group.
  - *cot\_prop*—Name of the COT property you want to modify.
  - *value*—Value for the specified COT property.
- Step 4** Save and activate your changes as described in the “Saving and Activating your Provisioning Changes” section on page 3-64.
- Step 5** Debug the COT settings on the associated media gateway using the **show cot dsp**, **show cot request**, **show cot summary**, and **debug cot detail** commands. Refer to the documentation for the associated media gateway for more information on these commands.
- If debugging the COT settings on the media gateway does not reveal any problems, or does not fix the COT failure, proceed to Step 6.
- Step 6** Contact the Cisco TAC to further analyze the problem and determine a solution. For more information about contacting the Cisco TAC, refer to the “Obtaining Technical Assistance” section on page xviii.

## Resolving an SRCP Audit Alarm

If an SRCP audit alarm should occur on your Cisco MGC, use the following procedure to resolve the problem:

- Step 1** Verify that the SRCP heartbeat is up and working.
- If the SRCP heartbeat is up and working, proceed to Step 2.
- If the SRCP heartbeat is not up and working, restart the SRCP heartbeat. If that does not resolve the alarm, proceed to Step 3.

- Step 2** Verify the configuration on the affected media gateway. The value in the field identified in the alarm should match the value given in the alarm description.
- If the configuration of your media gateway is incorrect, modify the configuration. The procedures for modifying the configuration of the media gateway can be found in the documentation for the media gateway.
- If the configuration of the media gateway is correct, proceed to Step 3.
- Step 3** Contact the Cisco TAC to further analyze the problem and determine a solution. For more information about contacting the Cisco TAC, refer to the “Obtaining Technical Assistance” section on page xviii.
- 

## Media Gateway IP Destination/Link Out-of-Service

If an IP link or destination to a media gateway is out-of-service, perform the following steps:



### Note

An IP destination to a media gateway is out-of-service when both IP links associated with the destination are out-of-service.

---

- Step 1** Ping the affected MGC link from the associated media gateway, using the following UNIX command:
- ```
ping link_addr
```
- Where *link_addr* is the IP address of the affected MGC link.
- Repeat this step if the second link for the destination is also out-of-service.
- If the links are unreachable, proceed to Step 2. Otherwise, proceed to Step 3.
- Step 2** If your system is using I/O cards to terminate the SS7 link, proceed to Step 3.
- If your system is using Cisco SLTs to terminate the SS7 link, proceed to Step 4.
- Step 3** If the path between the Cisco MGC and the media gateway is defined using an MGCP signaling service, proceed to Step 4. If the path between the Cisco MGC and the media gateway is defined using a NAS signaling service, proceed to Step 5.
- Step 4** Verify the MGCP interface on your media gateway is working properly. Refer to the documentation associated with the media gateway for more information.
- If the MGCP interface on your media gateway is working properly, proceed to Step x. Otherwise, correct the problems with the MGCP interface as described in the documentation associated with the media gateway.
- Step 5** Identify which Redundant Link Manager (RLM) group is configured on the media gateway by entering the **sh run** command. For more information on this command, refer to the documentation associated with the media gateway.
- Step 6** Verify that the RLM group identified in Step 5 is defined under the D-channel serial interface. Refer to the documentation associated with the media gateway for more information.
- If the RLM group is defined, proceed to Step 7. Otherwise, add the RLM group to the D-channel serial interface. Refer to the documentation associated with the media gateway for more information.
- If the link(s) returns to service, the procedure is complete. Otherwise, proceed to Step 7.
- Step 7** Reset the RLM group using the **shut/no shut** commands. Refer to the documentation associated with the media gateway for more information.

If the link(s) return to service, the procedure is complete. Otherwise, proceed to Step 8.

- Step 8** Verify that RLM messages are being acknowledged by the Cisco MGC using the **debug** command. Refer to the documentation associated with the media gateway for more information.

If RLM messages are being acknowledged by the Cisco MGC, proceed to Step 10. Otherwise, proceed to Step 9.

- Step 9** Verify that the configuration for RLM on the Cisco MGC matches the configuration on the media gateway. To display the configuration of the IP links on the Cisco MGC, enter the following MML command at the active Cisco MGC:

```
prov-rtrv:iplnk:"all"
```

The system returns a response similar to the following:

```
MGC-02 - Media Gateway Controller 2001-07-26 12:57:48
M RTRV
"session=active:iplnk"
/*
NAME          SVC          IF          IPADDR          PORT
PEERADDR      PEERPORT    PRI      SIGSLOT    SIGPORT    NEXTHOP    NETMASK
----          ---          --          -----          ----
-----
va-5300-202-1      va-5300-202      enif1      IP_Addr1      3001
172.24.200.19    3001              0              0      0.0.0.0    255.255.255.255
va-5300-202-2      va-5300-202      enif1      IP_Addr1      3001
172.24.200.19    3001              0              0      0.0.0.0    255.255.255.255
va-5300-203-1      va-5300-203      enif1      IP_Addr1      3001
172.24.200.20    3001              0              0      0.0.0.0    255.255.255.255
va-5300-203-2      va-5300-203      enif1      IP_Addr1      3001
172.24.200.20    3001              0              0      0.0.0.0    255.255.255.255
*/
```

Ensure that the IP addresses (IPADDR and PEERADDR) and the ports (PORT and PEERPORT) match the values used by the media gateway. If the values match, proceed to Step 10.

Otherwise, if the changes need to be made on the media gateway, refer to the documentation for your media gateway for more information. If the changes need to be made on the Cisco MGC, start a dynamic reconfiguration session to make your changes, as described in the “Invoking Dynamic Reconfiguration” section on page 3-65.

If the changes resolve the problem, the procedure is complete. Otherwise, proceed to Step 10.

- Step 10** Contact the Cisco TAC to further analyze the problem and determine a solution. For more information about contacting the Cisco TAC, refer to the “Obtaining Technical Assistance” section on page xviii.

CIC Mismatch (One-Way Audio)

If there is a mismatch between the CICs on your system and the far-end, perform the following steps:

- Step 1** Verify that the CIC numbering scheme on the far-end matches the settings on your Cisco MGC. To do this, log in to your active Cisco MGC, start an MML session, and enter the following command:

```
prov-rtrv:trnktype:"all"
```

Where *trnktype* is the type of trunk used on your system. Valid values are:

- nailedtrnk—Used in nailed trunk configurations, for the Cisco SC2200.

- switchtrnk—Used in switched trunk configurations, for the Cisco PGW 2200.

**Note**

The Cisco PGW 2200 PSTN Gateway was formerly known as the Cisco VSC3000 Virtual Switch Controller. Some parts of this document may use this older name.

For a nailed trunk configuration, the system returns a response similar to the following:

MGC-02 - Media Gateway Controller 2001-07-26 14:21:40

M RTRV

"session=active:nailedtrnk"

/*

| NAME | SRC SVC | SRC SPAN | SRC TIMESLOT (CIC) | DST SVC | DST SPAN | DST TIMESLOT (CIC) |
|------|---------|----------|--------------------|-------------|----------|--------------------|
| ---- | ----- | ----- | ----- | ----- | ----- | ----- |
| 1 | ss7svc1 | ffff | 1 | va-5300-202 | 0 | 1 |
| 2 | ss7svc1 | ffff | 2 | va-5300-202 | 0 | 2 |
| 3 | ss7svc1 | ffff | 3 | va-5300-202 | 0 | 3 |
| 4 | ss7svc1 | ffff | 4 | va-5300-202 | 0 | 4 |
| 5 | ss7svc1 | ffff | 5 | va-5300-202 | 0 | 5 |
| 6 | ss7svc1 | ffff | 6 | va-5300-202 | 0 | 6 |
| 7 | ss7svc1 | ffff | 7 | va-5300-202 | 0 | 7 |
| 8 | ss7svc1 | ffff | 8 | va-5300-202 | 0 | 8 |
| 9 | ss7svc1 | ffff | 9 | va-5300-202 | 0 | 9 |
| 10 | ss7svc1 | ffff | 10 | va-5300-202 | 0 | 10 |
| 11 | ss7svc1 | ffff | 11 | va-5300-202 | 0 | 11 |
| 12 | ss7svc1 | ffff | 12 | va-5300-202 | 0 | 12 |
| 13 | ss7svc1 | ffff | 13 | va-5300-202 | 0 | 13 |
| 14 | ss7svc1 | ffff | 14 | va-5300-202 | 0 | 14 |

For a switched trunk configuration, the system returns a response similar to the following:

MGC-100 - Media Gateway Controller 2001-07-30 09:47:28

M RTRV

"session=cotegress:switchtrnk"

/*

| NAME | SPAN | CIC | TRNKGRPNUM | CU | ENDPOINT |
|------|-------|-----|------------|---------|---------------------|
| ---- | ----- | --- | ----- | -- | ----- |
| 1 | ffff | 1 | 3005 | mgx-7-6 | vism/e1-1/1@mgx7-6 |
| 2 | ffff | 2 | 3005 | mgx-7-6 | vism/e1-1/2@mgx7-6 |
| 3 | ffff | 3 | 3005 | mgx-7-6 | vism/e1-1/3@mgx7-6 |
| 4 | ffff | 4 | 3005 | mgx-7-6 | vism/e1-1/4@mgx7-6 |
| 5 | ffff | 5 | 3005 | mgx-7-6 | vism/e1-1/5@mgx7-6 |
| 6 | ffff | 6 | 3005 | mgx-7-6 | vism/e1-1/6@mgx7-6 |
| 7 | ffff | 7 | 3005 | mgx-7-6 | vism/e1-1/7@mgx7-6 |
| 8 | ffff | 8 | 3005 | mgx-7-6 | vism/e1-1/8@mgx7-6 |
| 9 | ffff | 9 | 3005 | mgx-7-6 | vism/e1-1/9@mgx7-6 |
| 10 | ffff | 10 | 3005 | mgx-7-6 | vism/e1-1/10@mgx7-6 |
| 11 | ffff | 11 | 3005 | mgx-7-6 | vism/e1-1/11@mgx7-6 |
| 12 | ffff | 12 | 3005 | mgx-7-6 | vism/e1-1/12@mgx7-6 |
| 13 | ffff | 13 | 3005 | mgx-7-6 | vism/e1-1/13@mgx7-6 |
| 14 | ffff | 14 | 3005 | mgx-7-6 | vism/e1-1/14@mgx7-6 |

If these settings do not match those used by the far-end, start a dynamic reconfiguration session, as described in the “Invoking Dynamic Reconfiguration” section on page 3-65, and correct your settings. Otherwise, proceed to Step 2.

If that resolves the mismatch, the procedure is complete. Otherwise, proceed to Step 2.

- Step 2** Contact the Cisco TAC to further analyze the problem and determine a solution. For more information about contacting the Cisco TAC, refer to the “Obtaining Technical Assistance” section on page xviii.

Calls Fail at the Cisco MGC

If calls appear to be failing at the Cisco MGC, and the calls are not appearing on the associated media gateway, perform the following steps:

-
- Step 1** Debug the interface on the media gateway associated with the Cisco MGC. For media gateways associated with a Cisco SC2200, the interface is Q.931. For media gateways associated with a Cisco PGW 2200, the interface is MGCP. Refer to the documentation for the associated media gateway for more information on debugging the interface.
- If the calls in question do not appear on the media gateway, proceed to Step 2. Otherwise, resolve the problems with the interface as described in the documentation for the associated media gateway.
- Step 2** Verify that the signaling channels are in-service, as described in the “Retrieving Signaling Channel Attributes” section on page 3-48.
- If any of the signaling channels are out-of-service, attempt to bring them into service using the appropriate procedures. Otherwise, proceed to Step 3.
- Step 3** Run a call trace as described in the “Performing a Call Trace” section on page 8-102, and contact the Cisco TAC to further analyze the problem and determine a solution. For more information about contacting the Cisco TAC, refer to the “Obtaining Technical Assistance” section on page xviii.
-

Modifying Redundant Link Manager Timers

As of Release 7.4(12), you can modify the values of your Cisco MGC’s redundant link manager (RLM) timers. Refer to the *Release Notes for Cisco Media Gateway Controller Software* for more information.

If you want to change these timers, you must change them on the Cisco MGC and on the associated media gateway(s). To change the RLM timers, perform the following steps:



Note

RLM keepalives are sent only when traffic has not been transmitted for some time, that is, when a signaling message is received, the RLM keepalive timer is reset. RLM keepalives are sent by the media gateway to the Cisco MGC. If the RLM keepalive timer on the Cisco MGC expires, the system sets the IP link out-of-service. Increasing the RLM keepalive timer values on both sides can ensure that the IP link is not reset during transient conditions in the IP network, when the default values might be too stringent. However, if your system is in a continuous service configuration, increasing the values of the RLM keepalive timers reduces the system’s ability to quickly detect a link failure. Systems in a simplex configuration would not be affected.

- Step 1** Verify the current settings of your RLM timers on the Cisco MGC by logging in to the standby Cisco MGC, starting an MML session, and entering the following command:

```
prov-rtrv:lnksetprop:name="mgc_name"
```

Where *mgc_name* is the MML name of the Cisco MGC host.

The system returns a response similar to the following:

```
MGC-01 - Media Gateway Controller 2001-07-27 11:00:06
M   RTRV
    "session=active:lnksetprop"
    /*
linkEchoRetry = 3
```

```

linkLatencyTest = 600
linkOpenWait = 30
linkRecovery = 120
linkSwitch = 50
linkUpRecoveredMin = 600
port = 3000
PropagateSvcMsgBlock = false
timerCmdAck = 10
timerLinkDownMin = 100
timerLinkEcho = 10
unstableLink = 10
*/

```

All of the properties listed, except for port and PropagateSvcMsgBlock, are RLM timer properties.

Step 2 Start a provisioning session as described in the “Starting a Provisioning Session” section on page 3-63.

Step 3 Modify the RLM timer properties, as needed, using the following command:

```
prov-ed:lnkset:name="mgc_name",prop_name="value",prop_name="value",...
```

Where:

- *mgc_name*—The MML name of the Cisco MGC host.
- *prop_name*—The name of the RLM timer property you want to modify.
- *value*—The value you want for the specified RLM timer property.

Step 4 Save and activate your provisioning changes as described in the “Saving and Activating your Provisioning Changes” section on page 3-64.

Step 5 Reboot your system as described in the “Rebooting Your System to Modify Properties” section on page 8-124.

Tracing

Tracing on the Cisco MGC is described in the following sections:

- Performing a Call Trace, page 8-102
- Alternatives to Call Tracing, page 8-108
- Performing a TCAP Trace, page 8-111

Performing a Call Trace

After checking all physical connections, signal links, bearer channels, and destinations, the person who is troubleshooting the Cisco MGC begins to suspect that the call engine is part of the problem. Performing a call trace while making a call provides details about what is occurring inside the call engine and indicates where the breakdown is occurring (if it is occurring within the call engine).

Call tracing is described in the following sections:

- Starting A Call Trace, page 8-103
- Stopping A Call Trace, page 8-105
- Retrieving Names of Open Call Trace Files, page 8-105

- Viewing the Call Trace, page 8-105
- Deleting Call Trace Files, page 8-106
- Understanding the Call Trace, page 8-106

Starting A Call Trace

To start the call trace, perform the following steps:

Step 1 Log in to the active CiscoMGC, start an MML session, and enter the command.

This command can be entered in any one of five different formats:

1. `sta-sc-trc:sig_path:[log="filenameprefix"][,prd=n], confirm`
2. `sta-sc-trc:sig_path:span=x[,rng=y][,log="filenameprefix"][,prd=n]`
3. `sta-sc-trc:sig_path:span=x[,tc=z],rng=y[,log="filenameprefix"][,prd=n]`
4. `sta-sc-trc:trkgrp:[log="filenameprefix"][,prd=n], confirm`
5. `sta-sc-trc:trkgrp:trk=w[,rng=y][,log="filenameprefix"][,prd=n]`

Where:

- *sig_path*—The logical signaling destination, such as an SS7 point code, an FAS path, an IP FAS path, or a DPNSS path,
- *trkgrp*—The logical trunk group of interest.
- *filenameprefix*—Trace files are created and written to a file whose name can vary, depending on how the command is invoked. (A system log message is generated for each trace started. The filenames created as part of the **sta-sc-trc** command are contained in the log messages.) If the **log=** parameter is used, the value of this parameter is treated as a prefix to the filename.

If no **log=** parameter is used, default *filenameprefix* values are used for each **sta-sc-trc** command. For example:

- For **sta-sc-trc:sig_path:confirm** the filename is:

sig_path_yyyymmddhhmmss.btr

- For **sta-sc-trc:trkgrp:confirm** the filename is:

trkgrp_sig_path_yyyymmddhhmmss.btr

Where the filename (*yyymmddhhmmss*) is a time stamp, organized as follows:

- *yyyy*—Is the four-digit designation for the year, such as 2000, 2001, or 2002.
- *mm*—Is the two-digit designation for the month (01 through 12).
- *dd*—Is the two-digit designation for the day of the month (01 through 31).
- *hh*—Is the two-digit designation for the hour of the day (00 through 23).
- *mm*—Is the two-digit designation for the minutes (00 through 59).
- *ss*—Is the two-digit designation for the seconds (00 through 59).
- *n*—The duration for which call trace information is collected, in seconds. At the expiration of this period, the system discontinues PDU collection on the signaling path and closes the log file. In the absence of this parameter, the default period is set to 1800 seconds (30 minutes), after which time the trace is stopped automatically.

- **confirm**—An option that is required to confirm a *sig_path* level trace or a *trkgrp* level trace command. This is required due to the large volume of data that can be generated and the potential performance impact of generating a large trace file. If the confirm option is not entered, the command is rejected, and you receive a message regarding the potential performance impact of this command.
- *x*—The span ID, an integer value denoting the traffic channel for the *sig_path* (NFAS only).
- *y*—The range. When used with “**span=x**,” *y* is an optional range of spans beginning with span *x* and continuing for *y* spans. When used with “**tc=z**,” *y* is an optional range of traffic channels beginning with *z* and continuing for *y* traffic channels. When used with “**trk=w**,” *y* is an optional range of contiguous trunks to be traced starting with trunk *w* and ending with trunk *y*.
- *y*—The traffic channel of interest in integer form.
- *w*—The trunk of interest in integer form.

The following paragraphs present examples of each of the five possible command variations:

1. A signaling path level trace traces all calls occurring on the signaling path. Use this format if the specific traffic channel the call uses is unknown.

```
sta-sc-trc:sig_path:log="filenameprefix", prd=600, confirm
```

In this form of the command, the confirm parameter is required.

2. A signaling path/span level trace traces calls at the span level. Use this format to reduce the amount of trace information if you know the span on which the call will be placed.

```
sta-sc-trc:sig_path:span=x
```

The confirm parameter is not needed in this form of the command because the volume of the trace file should not be an issue, nor should system performance.

3. A signaling path/span/traffic channel level trace traces calls at the TC or CIC level. Use this format if the traffic channel on which the call will be placed is known.

```
sta-sc-trc:sig_path:span=x,tc=y
```

4. A trunk group level trace traces all calls at a trunk group level. Use this format if the trunk group on which the call will be placed is known.

```
sta-sc-trc:trkgrp:confirm
```

This form of the command requires the confirm parameter.

5. A trunk group/trunk level trace traces only calls for a given trunk (or CIC). Use this format if the trunk group and trunk on which the call will be placed is known.

```
sta-sc-trc:trkgrp:trk=w
```



Note

Refer to the *Cisco Media Gateway Controller Software Release 7 MML Command Reference Guide* for detailed information on using the **sta-sc-trc** command.

Step 2 Make the call.

Stopping A Call Trace

You can stop a call trace session using the **stp-sc-trc** MML command. To stop a call trace session on a particular signaling service, log in to the active Cisco MGC, start an MML session, and enter the following command:

```
stp-sc-trc:sig_srv|trkgrp
```

Where:

- *sig_srv*—MML name for the signaling service on which you are running a call trace.
- *trkgrp*—MML name for the trunk group on which you are running a call trace.

For example, to stop a call trace session on a trunk group called T-1-1, you would enter the following command:

```
stp-sc-trc:T-1-1
```

To stop all call trace sessions, log in to the active Cisco MGC, start an MML session, and enter the following command:

```
stp-sc-trc:all
```

The system returns a response similar to the following:

```
Media Gateway Controller 2000-03-21 15:28:03
M  COMPLD
    "ALL:Trace stopped for the following files:
    ../var/trace/_dpc1_20000321152752.btr
    "
```

Retrieving Names of Open Call Trace Files

To retrieve the names of call trace files for sessions that are in progress, log in to the active Cisco MGC, start an MML session, and enter the following command:

```
rtrv-sc-trc
```

The system returns a response similar to the following:

```
Media Gateway Controller 2000-03-21 15:28:03
M  RTRV
    "RTRV-SC-TRC:Trace in progress for the following files:
    ../var/trace/_dpc1_19991221131108.btr
    ../var/trace/sigtest_dpc2_19991221131109.btr
    "
```

Viewing the Call Trace

The MML command **sta-sc-trc** produces .btr (binary trace) files, which cannot be viewed with a text editor. The main part of the file name is set up in the **sta-sc-trc** command, as explained in the “Starting A Call Trace” section on page 8-103, and the Cisco MGC adds the .btr extension to these files. The .btr files can contain tracings from many calls all mixed together. Each tracing record in the file has a specific record type and records information of the type that relates to that record. Each record has a unique call ID that relates it to a specific call and is a recording of the external events that the MDL call model was exposed to while the recording was made. Each tracing record is not a recording of the actual MDL.

You can use the trace viewer to view and navigate through call trace outputs. For more information on using the trace viewer, refer to the “Using the Trace Viewer” section on page 3-117.

You can also view the call trace output data using the **get_trc.sh** UNIX script. **Get_trc.sh** uses the Conversion Analyzer and SimPrint utilities in combination to give a single common interface to all the trace tools. **Get_trc.sh** makes considerable use of the UNIX `less` utility for displaying file output and it is assumed that `less` is available on the system. You can start the script by entering the following UNIX command:

```
get_trc.sh filename
```

Where *filename* is the name of the call trace output data file (.btr) you want to view.

The script then displays a list of commands and prompts you to enter a command. The following commands are listed:

- S—Displays the call trace data using the SimPrint utility. For more information on SimPrint, refer to the “Understanding SimPrint” section on page 8-108.
- F—Displays the call trace data using the SimPrint utility, and a listing of the sent and received fields.
- D—Displays the data in the .trc file associated with this call trace. For more information on .trc files, refer to the “Understanding Trace Files” section on page 8-108.
- C—Converts the file created by this script to a .trc file.
- A—Displays the data in the .ca file associated with this call trace. For more information on .ca files, refer to the “Understanding the Conversion Analyzer” section on page 8-107.
- N—Displays the information for the next call ID in the list.
- P—Displays the information for the previous call ID in the list.
- L—Lists all of the call IDs in the data for this call trace.
- H—Provides help on displaying call trace data.
- Q—Closes the script.
- id—Displays the information for a call ID that you specify.

Deleting Call Trace Files

Call trace files can be rather large, and leaving these files on your disk after you no longer require them could raise capacity issues. Call trace files are deleted using UNIX commands, as described in the “Deleting Unnecessary Files to Increase Available Disk Space” section on page 8-112.

Understanding the Call Trace

Call traces record information in a trace file that shows how the Cisco MGC processed a specific call. Traces are most useful when you can be sure that a problem call is reaching the call engine and starting an instance of a Message Definition Language (MDL) state machine. You can determine whether the problem call is reaching the call engine by looking for the presence of non-idle circuits (**rtrv-cic**) or “new cmgCall” entries in the debug logs.

After you start a trace, all call-processing activity for calls originating from the specified destination is captured. This allows you to follow the call through the Cisco MGC to see where it fails.

The trace output is in binary format. It shows:

- The PDU that the Cisco MGC receives
- How the Cisco MGC decodes the PDU

- The PDU that the Cisco MGC sends out

Using call trace logs is easy if you remember how to locate the record of a call:

- You can easily locate incoming signal messages that cause instances of engine call objects to be started by searching backwards in the call trace for “new cmgCall.”
- Similarly, you can find the end of a call by searching forward from the “new cmgCall” message for the next “end cmgCall” message.

If you are experiencing problems with call processing and need to contact Cisco for support, you should run a call trace before contacting Cisco's TAC. The trace file helps the Cisco TAC troubleshoot the problem more effectively. For some problems, the Cisco TAC cannot begin troubleshooting the problem until you supply the trace file, so it is a good practice to create this file before contacting them.

Understanding the Conversion Analyzer

The Conversion Analyzer is a viewer utility for .btr trace files. The Conversion Analyzer displays each record from a .btr file in a readable form (ASCII text) that can be viewed with any text editor; however, some useful sorting and display options are also available.

The .btr files serve as source files for .ca files. The .ca files are ASCII text output from the Conversion Analyzer obtained by redirection of the standard output to a file. There are two main sections in a .ca file. The header section contains a list of every signaling path defined on the Cisco MGC and a list of the message definition object (MDO) modules that are loaded. The main body contains a printout of every record. Each record has a record number, a timestamp, a call ID, and the print data that the record contains.

Understanding the Simulator Utility

The Simulator is a powerful MDO file processing utility that uses .mdo files to replay the events recorded in a .btr file. The front end of the Simulator reads the .btr file. The interpreter in the Simulator utility that loads the .mdo files and replays the events (.btr files) through the MDO, is the same interpreter used by the call engine in the Cisco MGC when .mdo files are used. As the interpreter steps through each line of object code (and the action of each object is interpreted) in the .mdo file, each object's print method is activated, which forms the next line of text in the .trc file.

The print method for each object contains text that directly relates to the appearance of the .mdl source code that produced the object in the .mdo file (through compilation of the .mdl source code with the MDL compiler). The .mdo files used with the Simulator when it is processing a .btr file to create a .trc file, must be the same .mdo files that were in use when the .btr file was originally recorded on the Cisco MGC. This is why the conversion from a .btr file to a .trc file is usually done on the Cisco MGC that originated the .btr file.

The interpreter is not used with .so files because those files interact directly with the call engine in the Cisco MGC, but the tracer can record a .btr file regardless of whether .mdo or .so files were used to process the call. The Simulator can, however, replay .btr files using .so files in place of .mdo files. This is a way of checking that the .so and .mdo files perform in exactly the same way, although .so is faster.

Because .so files do not contain MDO objects, there are no print methods available to the Simulator, so no .trc output is possible. When a .btr file is produced by a Cisco MGC using .so files, the replay in the Simulator must be done with the .mdo files that were used to produce the .so files in order to produce an accurate .trc file.

Understanding Trace Files

Trace files (.trc files) are text files that are produced by the Simulator utility. They contain detailed line by line trace information from the MDO code that was run in the simulation replay that produced the file, thus they contain MDL traces. The .trc extension is added by the `get_trc.sh` script if the source of the trace is a .btr file.

Trace files are source files for the SimPrint (SP) utility. They are text files and can be viewed with a text editor. The .trc file should be sent to Cisco TAC if expert analysis is required.

Understanding SimPrint

SimPrint (SP) is a viewing utility for .trc files. SP converts a .trc file into a sequence diagram that shows all of the external and internal events that occur in a .trc file. This is useful for getting an overview of what is occurring in the trace.

The following list defines the terms used in the call flow printouts generated by the SimPrint tool:

- **LINE**—Refers generically to the incoming and outgoing interfaces of the Cisco MGC.
- **OCC**—Originating Call Control state machine. The call is passed from the incoming interface to a protocol adapter, where it is converted into a generic message signaling unit (MSU) and sent to the OCC for parsing of MSU data to memory.
- **LCM**—Lightspeed Call Model state machine. The LCM is a generic call model containing event handlers to process generic call event data. This processing includes generic call analysis, requests for bearer channels, and transfer of the MSU to the appropriate TCC state machine. The LCM is also known as the Universal Call Model (UCM).
- **ANALYSIS**—The LCM can perform generic call analysis, based on the content of the MSU. The LCM exchanges data with the call processing engine to analyze the MSU. After analysis is complete, an available circuit is identified and the LCM sends a bearer channel seizure request message to the CPM state machine.
- **CPM**—Connection Plane Manager state machine. The CPM exchanges data with the call processing engine to seize and prepare a bearer channel for routing of the call data.
- **CDR**—Call Detail Record. CDR information is created as a result of LCM processing of the MSU.
- **TRIGGER**—Intelligent Network (IN) Trigger state machine. This state machine is used to send and receive IN trigger events to the Transfer Capabilities Application Part (TCAP) interface in the I/O channel controller (IOCC). This enables IN messages to be sent to a service control point (SCP).
- **ENGINE**—The call processing engine exchanges data with the LCM as generic call analysis is performed on the MSU and a bearer channel is seized and prepared for routing of the call data.
- **TCC**—Terminating Call Control state machine. The TCC changes the call data into a protocol-specific protocol data unit (PDU) and passes the PDU to the terminating IOCC for routing to the outgoing interface.

Alternatives to Call Tracing

Performing call traces to identify problems can be difficult due to the large amount of data the trace may gather before the error occurs, and the negative impact performing call traces has on system performance. The Cisco MGC software has MML commands that can be used to diagnose problems with hung calls and abnormal call termination. The following sections describe those commands.

Diagnosing Hung Calls

You can print the diagnostic information about hung calls to a file using the **prt-call** MML command. The contents of the file include all of the previous states of the call and a history of occurrences leading up to the call being stuck in its current state.

To print diagnostic information on a hung call, complete the following steps:

Step 1 Log in to the active Cisco MGC and enter the following command:

```
prt-call:sig_path:cic=number [,log=xyz]
```

or

```
prt-call:sig_path:span=phys, bc=bchan [,log=xyz]
```

Where:

- *sig_path*—Corresponding MML name for any of the following component types:
 - Signaling path of in-band TDM up to MUX and then time switched to TDM media and sent to Cisco MGC.
 - Signaling path of in-band TDM signaling up to CU and then encapsulated and sent over IP to the Cisco MGC.
 - Signaling path of in-band TDM signaling up to NAS and then converted to NI2 and sent to the Cisco MGC over IP (that is, FE box<-sig/tdm->NAS<-NI2/IP->Cisco MGC).
 - Signaling path or routeset associated with SS7 destination point code.
 - Signaling path for EISUP.



Note This command allows for the use of wildcards for the *sig_path* parameter.

- *number*—A numeric value that identifies the ISUP circuit identification code (CIC) number.
- *phys*—A 16-bit value that identifies an ISDN/PRI physical cable.
- *bchan*—A numeric value that identifies the non-ISUP bearer channel number. BC is used for non-ISUP trunks.; otherwise use CIC.
- *xyz*—The name of an ASCII log file to which the output of this command is written. The name given in this parameter is used as a prefix to the actual name of the file, which includes the *sig_path* name, date, and time. If no log file name is provided, a default name consisting of the *sig_path* name, date, and time is created. The extension of these log files is .prt, and they are located in the \$BASEDIR/var/trace directory.

For example, the following MML command prints call data for a signaling path called dms100-pc using a CIC of 124:

```
prt-call:dms100-pc:cic=124
```

The output for this command is stored in a file called pc_timestamp.prt, where *timestamp* is the time of the file's creation.

Step 2 To change directories, enter the following command:

```
cd /opt/CiscoMGC/var/trace
```

- Step 3** Use a text file viewer, such as vi, to view the contents of the log file.

Performing an Abnormal Call Termination Trace

You can print the global variable information from the state machine and external event information for a call to a file using the **sta-abn-trc** MML command. To print this information, complete the following steps:

- Step 1** Log in to the active Cisco MGC, start an MML session, and enter the following command:

```
sta-abn-trc:sig_path|all[,log=xyz] [,prd=n],confirm
```

Where:

- *sig_path*—Corresponding MML name for any of the following component types:
 - Signaling path of in-band TDM up to MUX and then time switched to TDM media and sent to Cisco MGC.
 - Signaling path of in-band TDM signaling up to CU and then encapsulated and sent over IP to the Cisco MGC.
 - Signaling path of in-band TDM signaling up to NAS and then converted to NI2 and sent to the Cisco MGC over IP (that is, FE box<-sig/tdm->NAS<-NI2/IP->Cisco MGC).
 - Signaling path or routeset associated with SS7 DPC.
 - Signaling path for EISUP.



Note This command allows for the use of wildcards for the *sig_path* parameter.

- **all**—Indicates that the start trace command needs to be applied to the whole Cisco MGC, in which case only one trace file is generated.
- *xyz*—The name of an ASCII log file to which the output of this command is written. The name given in this parameter is used as a prefix to the actual name of the file, which includes the *sig_path* name, date, and time. If no log file name is provided, a default name consisting of the *sig_path* name, date, and time is created. The extension of these log files is .prt, and they are located in the \$BASEDIR/var/trace directory.
- *n*—The period, in seconds, for which this trace is enabled, during which time any abnormal calls are traced. If this optional parameter is not used, the period defaults to 30 seconds.

For example, the following MML command prints call data for a signaling path called dms100-pc to a file named trace1 (since the period parameter, *n*, is not entered, the trace lasts for the default period, 30 seconds):

```
sta-abn-trc:dms100-pc,log=trace1,confirm
```

- Step 2** To change directories, enter the following UNIX command:

```
cd /opt/CiscoMGC/var/trace
```

- Step 3** Use a text file viewer, such as vi, to view the contents of the log file.

Stopping an Abnormal Call Termination Trace

You can stop an in-progress abnormal call termination trace using the **stp-abn-trc** MML command. To do this, log in to the active Cisco MGC, start an MML session, and enter the following command:

```
stp-abn-trc:sig_srv
```

Where *sig_srv* is the MML name for a signaling service on which an abnormal call termination trace is being run.

For example, to stop an abnormal call termination trace being run on a signaling service called *ss7srv1*, you would enter the following command:

```
stp-abn-trc:ss7srv1
```

The system responds with a response similar to the following:

```
Media Gateway Controller 2000-05-26 07:02:11
M  COMPLD
"Trace stopped for the following file:

../var/trace/_20000526070211.abn
"
```

To stop all in-progress abnormal call termination traces, log in to the active Cisco MGC, start an MML session, and enter the following command:

```
stp-abn-trc:all
```

The system returns a response similar to the following:

```
Media Gateway Controller 2000-05-26 07:02:11
M  COMPLD
"ALL:Trace stopped for the following files:

../var/trace/_20000526070211.abn
"
```

Performing a TCAP Trace

To run a TCAP trace on your system, perform the following steps:

-
- | | |
|---------------|--|
| Step 1 | Start the TCAP trace by logging in to the active Cisco MGC, starting an MML session, and entering the following command:

<pre>sta-tcap-trc</pre> |
| | The system begins sending TCAP trace messages to the active system logs file. |
| Step 2 | View the active system logs file, as described in the “Viewing System Logs” section on page 8-4. Make note of any TCAP trace messages, such as hex dumps of messages sent to the SCCP layer. |
| Step 3 | When your TCAP trace is complete, enter the following command to stop the TCAP trace:

<pre>stp-tcap-trc</pre> |
-

Platform Troubleshooting

The following sections contain procedures related to resolving problems with the Cisco MGC platform:

- Deleting Unnecessary Files to Increase Available Disk Space, page 8-112
- Recovering from a Switchover Failure, page 8-113
- Recovering from Cisco MGC Host(s) Failure, page 8-115
- Restoring Stored Configuration Data, page 8-117
- Verifying Proper Configuration of Replication, page 8-123
- Measurements Are Not Being Generated, page 8-123
- Call Detail Records Are Not Being Generated, page 8-123
- Rebooting Your System to Modify Properties, page 8-124
- Rebooting Software to Modify Configuration Parameters, page 8-125
- Resolving a Failed Connection to a Peer, page 8-125

Deleting Unnecessary Files to Increase Available Disk Space

You may need to delete call trace files, archived log files, or configurations from your system to create more available disk space on your Cisco MGC.

The following procedure steps you through the process of deleting all three file types.

- Step 1** Log in to the active Cisco MGC and enter the following UNIX commands to determine whether the affected disk drive contains any call trace files in the /opt/CiscoMGC/var/trace directory:

```
cd /opt/CiscoMGC/var/trace
```

```
ls
```

The system responds with a list of files in the directory. If the command response indicates that there are *.btr and *.trc files stored in this directory, then proceed to Step 2. Otherwise, proceed to Step 4.



Note Do not delete any call trace files related to troubleshooting any current system problems.

- Step 2** Delete the identified call trace files using the following UNIX command:

```
rm -i filename
```

Where *filename* is the name of the call trace file (either *.btr or *.trc) you have identified for deletion.

- Step 3** Repeat Step 2 for each additional call trace file identified for deletion.

- Step 4** Enter the following UNIX commands to view the archived logs in the /opt/CiscoMGC/var/spool directory on the affected disk drive:

```
cd /opt/CiscoMGC/var/spool
```

```
ls
```

The system responds with a list of files in the directory. Review the listed files. If there are archived log files listed that are no longer required, proceed to Step 5. Otherwise, proceed to Step 7.



Note If you are backing up your system software on a regular basis, you can retrieve any files that you choose to delete from your backup files, if the need arises. For more information on backing up your system software, refer to the “Backing Up System Software” section on page 3-28.

Step 5 Delete the identified archived log files using the following UNIX command:

```
rm -i filename
```

Where *filename* is the name of the archived log file you have identified for deletion.

Step 6 Repeat Step 5 for each additional identified archived log file.

Step 7 Use the config-lib viewer to view the contents of the configuration library, using the information in the “Using the Config-Lib Viewer” section on page 3-113. Determine whether any of the configurations listed are no longer necessary for the operation of your system. If any of the configurations can be deleted, delete them using the information in the “Using the Config-Lib Viewer” section on page 3-113.

Recovering from a Switchover Failure

Use the procedure in this section to recover from a failed switchover operation. You would typically use this procedure when the standby Cisco MGC is unavailable to process calls and a critical alarm occurs on the active Cisco MGC.

To recover from a switchover failure, complete the following steps:

Step 1 Log in to the active Cisco MGC, start an MML session, and view the current alarms, as described in the “Retrieving All Active Alarms” section on page 8-3.

Step 2 Identify the critical alarm that caused the switchover attempt. To do this, review the alarm(s) that are listed in the response. There should be at least one critical alarm, and an alarm indicating that a switchover began and another alarm indicating that the switchover failed.

If there is only one critical alarm listed, that alarm caused the switchover attempt.

If there is more than one critical alarm listed, compare the timestamp of the critical alarms with the timestamp of the alarm indicating that a switchover began. The critical alarm that occurred before the switchover was begun is the alarm that caused the switchover attempt.

Step 3 Refer to the “Alarm Troubleshooting Procedures” section on page 8-8 for descriptions of the steps necessary to resolve the critical alarm that caused the switchover attempt.

Step 4 Log in to the standby Cisco MGC, start an MML session, and view the current alarms, as described in the “Retrieving All Active Alarms” section on page 8-3.

Step 5 Resolve the listed alarm(s). Refer to the “Alarm Troubleshooting Procedures” section on page 8-8 for descriptions of the steps necessary to resolve the alarm(s).

If resolving the alarms does not stabilize the standby Cisco MGC, proceed to Step 6.

Step 6 Generate a ping from the active Cisco MGC to the standby Cisco MGC by entering the following UNIX command at the active Cisco MGC:

```
ping standby_addr
```

Where *standby_addr* is the IP address of the standby Cisco MGC.

If the ping fails, proceed to Step 7. Otherwise, proceed to Step 8.

- Step 7** Verify the Ethernet interfaces between the active Cisco MGC and the standby Cisco MGC. Refer to the Sun Microsystems documentation that came with your system for more information.

If an element of the Ethernet interfaces between the active Cisco MGC and the standby Cisco MGC is found to be faulty, replace it. Otherwise, proceed to Step 8. Refer to the Sun Microsystems documentation that came with your system for more information.

If that resolves the problem, the procedure is complete. Otherwise, proceed to Step 8.

- Step 8** Verify that the host name for each Cisco MGC host is unique. To do this, log on as root to each Cisco MGC host and view the contents of the host file in the /etc directory. If a Cisco MGC host does not have a unique host name, enter the following UNIX command:

```
# echo host_name > /etc/host
```

Where *host_name* is a unique name for the Cisco MGC host.

- Step 9** Verify that the IP address parameters in the XECfgParm.dat file, which are listed below, are set correctly on each host.

- *.ipAddrLocalA
- *.ipAddrLocalB
- *.ipAddrPeerB
- *.IP_Addr1
- *.IP_Addr2
- *.IP_Addr3
- *.IP_Addr4

If the IP address settings are correct, proceed to Step 10. Otherwise, update the IP address parameters for each host, using the procedure in the “Rebooting Software to Modify Configuration Parameters” section on page 8-125.

If that resolves the problem, the procedure is complete. Otherwise, proceed to Step 10.

- Step 10** Verify that the settings for the foverd parameters are set correctly in the XECfgParm.dat file, which are listed below, on each host.

```
foverd.conn1Type      = socket
foverd.ipLocalPortA   = 1051
foverd.ipPeerPortA    = 1052
foverd.conn2Type      = socket
foverd.ipLocalPortB   = 1053
foverd.ipPeerPortB    = 1054
foverd.conn3Type      = serial
foverd.conn3Addr      = /dev/null
foverd.abswitchPort   = (/dev/null)
foverd.heartbeatInterval = 4000
```

If the foverd settings are correct, proceed to Step 11. Otherwise, update the foverd settings in the XECfgParm.dat files using the procedure in the “Rebooting Software to Modify Configuration Parameters” section on page 8-125.

If that resolves the problem, the procedure is complete. Otherwise, proceed to Step 11.

- Step 11** Contact the Cisco TAC to further analyze the problem and determine a solution. For more information about contacting the Cisco TAC, refer to the “Obtaining Technical Assistance” section on page xviii.
-

Recovering from Cisco MGC Host(s) Failure

There are situations, such as a replacement of a failed disk drive, natural or man-made disaster, or software corruption, that make it necessary for you to recover the software configuration data for a failed Cisco MGC host or hosts. (for example, if the Cisco MGC software has become corrupted or you have replaced a failed disk drive).

**Note**

In these procedures, it is assumed that backup operations have been performed regularly on your Cisco MGC. For more information on backing up your Cisco MGC, refer to the “Backing Up System Software” section on page 3-28.

**Note**

Successful recovery from a natural or man-made disaster depends upon your planning in advance for a possible disaster. Refer to the “Creating a Disaster Recovery Plan” section on page 3-27 for more information.

The following sections contain the procedures that describe how to recover from Cisco MGC host(s) failure:

- Recovering from a Cisco MGC Host Failure in a Simplex System, page 8-115
- Recovering from a Single Cisco MGC Host Failure in a Continuous Service System, page 8-116
- Recovering from a Dual Cisco MGC Host Failure in a Continuous Service System, page 8-116

Recovering from a Cisco MGC Host Failure in a Simplex System

To recover from a Cisco MGC host failure in a system equipped with only one Cisco MGC, perform the following steps:

-
- Step 1** Reload the Solaris 2.6 operating system on the Cisco MGC host, as described in the *Installing the Operating System Software* chapter of the *Cisco Media Gateway Controller Software Release 7 Installation and Configuration Guide*.
- Step 2** Reload the Cisco MGC software on the Cisco MGC host, as described in the *Installing the Cisco Media Gateway Controller Software* chapter of the *Cisco Media Gateway Controller Software Release 7 Installation and Configuration Guide*.
- Step 3** Restore the configuration of your Cisco MGC from your latest backup file, as described in the “Restoring Stored Configuration Data” section on page 8-117.

**Note**

If your backup files are stored on a remote server, have your network administrator re-establish the path between the Cisco MGC and the server that stores your backups.

**Note**

Any changes you made to the Cisco MGC system subsequent to your last backup are lost.

- Step 4** Start the Cisco MGC software, as described in the “Starting the Cisco MGC Software” section on page 2-2.

Recovering from a Single Cisco MGC Host Failure in a Continuous Service System

To recover from a single Cisco MGC host failure in a system equipped with two Cisco MGCs, perform the following steps:

- Step 1** Reload the Solaris 2.6 operating system on the affected Cisco MGC host, as described in the *Installing the Operating System Software* chapter of the *Cisco Media Gateway Controller Software Release 7 Installation and Configuration Guide*.
- Step 2** Reload the Cisco MGC software on the affected Cisco MGC host, as described in the *Installing the Cisco Media Gateway Controller Software* chapter of the *Cisco Media Gateway Controller Software Release 7 Installation and Configuration Guide*.
- Step 3** Restore the configuration of the affected Cisco MGC from your latest backup file, as described in the “Restoring Stored Configuration Data” section on page 8-117.

**Note**

If your backup files are stored on a remote server, have your network administrator re-establish the path between the affected Cisco MGC and the server that stores your backups.

- Step 4** Open the XECfgParm.dat file on the affected Cisco MGC in a text editor, such as vi.
- Step 5** Search for the pom.dataSync property and ensure that it is set to *true*.
- Step 6** Save the file and exit the text editor.
- Step 7** Start the Cisco MGC software, as described in the “Starting the Cisco MGC Software” section on page 2-2.
- Step 8** Contact the Cisco TAC for assistance in synchronizing the databases of the active and standby Cisco MGCs. Refer to the “Obtaining Technical Assistance” section on page xviii for more information on contacting the Cisco TAC.h

Recovering from a Dual Cisco MGC Host Failure in a Continuous Service System

To recover from a dual Cisco MGC host failure in a system equipped with two Cisco MGCs, perform the following steps:

- Step 1** Select one of the Cisco MGC hosts to be your active system, and the other to be your standby system.
- Step 2** Reload the Solaris 2.6 operating system on the active Cisco MGC host, as described in the *Installing the Operating System Software* chapter of the *Cisco Media Gateway Controller Software Release 7 Installation and Configuration Guide*.

Step 3 Reload the Cisco MGC software on the active Cisco MGC host, as described in the *Installing the Cisco Media Gateway Controller Software* chapter of the *Cisco Media Gateway Controller Software Release 7 Installation and Configuration Guide*.

Step 4 Restore the configuration of the active Cisco MGC from your latest backup file, as described in the “Restoring Stored Configuration Data” section on page 8-117.



Note If your backup files are stored on a remote server, have your network administrator re-establish the path between the active Cisco MGC and the server that stores your backups.

Step 5 Open the XECfgParm.dat file on the active Cisco MGC in a text editor, such as vi.

Step 6 Search for the pom.dataSync property and ensure that it is set to *true*.

Step 7 Save the file and exit the text editor.

Step 8 Start the Cisco MGC software on the active Cisco MGC, as described in the “Starting the Cisco MGC Software” section on page 2-2.

Step 9 Reload the Solaris 2.6 operating system on the standby Cisco MGC host, as described in the *Installing the Operating System Software* chapter of the *Cisco Media Gateway Controller Software Release 7 Installation and Configuration Guide*.

Step 10 Reload the Cisco MGC software on the standby Cisco MGC host, as described in the *Installing the Cisco Media Gateway Controller Software* chapter of the *Cisco Media Gateway Controller Software Release 7 Installation and Configuration Guide*.

Step 11 Restore the configuration of the standby Cisco MGC from your latest backup file, as described in the “Restoring Stored Configuration Data” section on page 8-117.



Note If your backup files are stored on a remote server, have your network administrator re-establish the path between the standby Cisco MGC and the server that stores your backups.

Step 12 Open the XECfgParm.dat file on the standby Cisco MGC in a text editor, such as vi.

Step 13 Search for the pom.dataSync property and ensure that it is set to *true*.

Step 14 Save the file and exit the text editor.

Step 15 Start the Cisco MGC software, as described in the “Starting the Cisco MGC Software” section on page 2-2.

Step 16 Contact the Cisco TAC for assistance in synchronizing the databases of the active and standby Cisco MGCs. Refer to the “Obtaining Technical Assistance” section on page xviii section for more information on contacting the Cisco TAC.

Restoring Stored Configuration Data

Typically, restoration of stored configuration data is performed in severe troubleshooting situations where the Cisco MGC is not functioning properly, due to hardware failure, natural disaster, or software corruption. The procedures in this section describe how to restore the Cisco MGC configuration data stored either on a tape drive or on a remote network server.

There are two restoration methods available for the Cisco MGC software, one for software releases up to 7.4(10), and another for software releases from 7.4(11) and above. These restoration procedures are mutually exclusive. You cannot use the restoration procedures for one software release to restore files backed up using the procedures specific to the other release.

These restoration methods are described in the following sections:

- Restoring Procedures for Cisco MGC Software up to Release 7.4(10), page 8-118
- Restoring Procedures for Cisco MGC Software Release 7.4(11) and up, page 8-121

Restoring Procedures for Cisco MGC Software up to Release 7.4(10)

This restoration method uses a script to restore the configuration data for the Cisco MGC software from either a local tape drive or on to a remote machine. Restoration of the Main Memory Database (MMDB) is performed by a separate script.

The following sections provide the restoration procedures:

- Restoring Data from a Local Tape Drive, page 8-118
- Restoring Data from a Remote Machine over the Network, page 8-119
- Restoring Data to the Main Memory Database, page 8-121



Note

These procedures assume that you have backed up your system configuration data regularly. The procedures for system configuration backup can be found in the “Backup Procedures for Cisco MGC Software up to Release 7.4(10)” section on page 3-28.

Restoring Data from a Local Tape Drive

This procedure restores everything on a tape in a local tape drive to the Cisco MGC base directory.



Caution

This procedure overwrites existing files under the Cisco MGC base directory. Current content in the overwritten files will be lost!

To restore the contents of the entire Cisco MGC software directory from a local tape, complete the following steps:

Step 1 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/mm1.log, 187 bytes, 1 tape blocks.
.
.
.
#
```

- Step 4** When the restore has finished, remove the tape from the tape drive.
- Step 5** If you have performed any partial backups since the creation of the full backup tape you have just restored, retrieve the most recent partial backup tape and repeat steps 1 to 4 with that tape in the tape drive.
- Step 6** 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 8-121.

Restoring Data from a Remote Machine over the Network

This procedure restores files to the Cisco MGC software base directory from a file on an NFS mountable directory on a remote machine. The remote machine must be set up with an NFS mountable directory that can be written to by the machine being backed up. The NFS setup of the remote machine is beyond the scope of this procedure.

To restore the contents of the Cisco MGC software directory from a remote machine, complete the following steps:

- Step 1** 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 you have performed any partial backups since the creation of the full backup you have just restored, repeat Steps 1 to 7 and restore the most recent partial backup.
- Step 9** 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 8-121.

Restoring Data to the Main Memory Database

Use this procedure to restore dial plan data, which was stored in the MMDB, in a single file as described in the “Performing a Backup Operation on the Main Memory Database” section on page 3-32.

- Step 1** Log in to the active Cisco MGC and 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** Stop the MMDB by entering the following UNIX command:

```
ttreplic
```

- Step 3** 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
```

- Step 4** Restore the MMDB by entering the following UNIX command:

```
ttreplic
```

Restoring Procedures for Cisco MGC Software Release 7.4(11) and up

This restoration method uses a script to restore the configuration data for the Cisco MGC software, select UNIX administrative files, and the Main Memory Database (MMDB).

**Note**

This functionality is part of a patch to Release 7.4(11). If you want to use this functionality, you must be upgraded to the proper patch level. For more information on verifying the patch level of your system, refer to “Verifying the Patch Level of the Cisco MGC” section on page 3-104.

The following sections provide the restoration procedures:

- Restoring Data from a Local Tape Drive, page 8-118
- Restoring Data from a Remote Machine over the Network, page 8-119

**Note**

These procedures assume that you have backed up your system configuration data regularly. The procedures for system configuration backup can be found in the “Backup Procedures for Cisco MGC Software from Release 7.4(11) and up” section on page 3-33.

Listing Backup Files

To list the backup files in a particular directory path, enter the following UNIX command on the Cisco MGC:

```
mgcrestore -d path -l
```

Where *path* is the directory path in which you have stored backup files, such as a directory on a remote server or a local tape drive.

The system returns a response similar to the following:

```
Backup files in /var/cisco
```

```
-----  
mgc_venus_20011010_153003_backup.tar  
mgc_venus_20011011_153003_backup.tar  
mgc_venus_20011012_153003_backup.tar
```

Restoring a Backup File

To restore the configuration data stored in a particular backup file, enter the following UNIX command on the affected Cisco MGC to run the restore script:

```
mgcrestore -d path -f filename
```

Where:

- *path*—The directory path to the location where your backup files are stored.
- *filename*—The file name of the backup file you want to restore.

For example, to restore a backup file called `mgc_venus_20011012_153003_backup.tar` stored in a directory path called `/var/cisco`, you would enter the following command:

```
mgcrestore -d /var/cisco -f mgc_venus_20011012_153003_backup.tar
```


Verifying Proper Configuration of Replication

If calls are not being preserved when your system performs a switchover, you should verify that your system is properly configured for replication of call data. To do this, verify that the value of the parameters in the XECfgParm.dat file on each host match the settings listed below, using the procedure in the “Rebooting Software to Modify Configuration Parameters” section on page 8-125.

```
*.SyscheckpointEnabled = true
replicator.portDataChannelSend = 2968
replicator.portDataChannelRecv = 2970
replicator.portCommChannelSend = 2972
replicator.portCommChannelRecv = 2974
replicator.reconnectInterval = 15
replicator.numberReadThreads = 1
```

Measurements Are Not Being Generated

If your Cisco MGC is not generating system measurements, perform the following procedure:

-
- Step 1** Verify that the amdmp process is running, as described in the “Verifying That Processes Are Running” section on page 3-3.
- If the amdmp process is not running, proceed to Step 2. Otherwise, proceed to Step 3.
- Step 2** Verify that the *.disableMeas parameter in the XECfgParm.dat file is set to *false* on each host, using the procedure in the “Rebooting Software to Modify Configuration Parameters” section on page 8-125.
- Step 3** Contact the Cisco TAC to further analyze the problem and determine a solution. For more information about contacting the Cisco TAC, refer to the “Obtaining Technical Assistance” section on page xviii.
-

Call Detail Records Are Not Being Generated

If call detail records are not being generated on your Cisco MGC, perform the following steps:

-
- Step 1** Verify that the dmpr-01 process is running, as described in the “Verifying That Processes Are Running” section on page 3-3.
- If the dmpr-01 process is not running, proceed to Step 2. Otherwise, proceed to Step 4.
- Step 2** Verify that the settings for the dmprSink.dat file are correct, using the procedure in the “Configuring the Data Dumper” section on page A-2.
- If that clears the alarm, the procedure is finished. Otherwise, proceed to Step 3.
- Step 3** Verify that the settings for the CDR parameters in the XECfgParm.dat file on each host match those listed below, using the procedure in the “Rebooting Software to Modify Configuration Parameters” section on page 8-125.

```
cdrDmpr.openCDR          = true
cdrDmpr.callDetail        = /opt/CiscoMGC/local/cdbscript.sh
cdrDmpr.seqFile           = ../var/.cdr.seq
diskmonitor.CdrRmFinished = 0      # remove "finished" cdrs after X days (0 = immediate)
engine.CDRencodingFormat  = AnsiCDB
engine.CDRtimeStamp       = S
```

```
engine.CDRmessageTypes = "1010,1020,1030,1040,1050,1060,1070"
```

- Step 4** Contact the Cisco TAC to further analyze the problem and determine a solution. For more information about contacting the Cisco TAC, refer to the “Obtaining Technical Assistance” section on page xviii.
-

Rebooting Your System to Modify Properties

When you are modifying certain properties on the Cisco MGC, it is required that you reboot your system as part of the modification process. To reboot your system as part of a property modification process, perform the following steps:

-
- Step 1** Log in to your active Cisco MGC and change directories to the /opt/CiscoMGC/etc directory using the following UNIX command:
- ```
cd /opt/CiscoMGC/etc
```
- Step 2** Open the XECfgParm.dat file in a text editor, such as vi.
- Step 3** Search for the pom.dataSync property and ensure that it is set to *false*.
- Step 4** Save the file and exit the text editor.
- Step 5** Shut down the Cisco MGC software on your active Cisco MGC, as described in the “Shutting Down the Cisco MGC Software Manually” section on page 2-4. This causes the currently standby Cisco MGC to become the active Cisco MGC.
- Step 6** Start the Cisco MGC software on the Cisco MGC, as described in the “Starting the Cisco MGC Software” section on page 2-2.
- Step 7** Once the Cisco MGC software is fully activated, log in to the active Cisco MGC and perform a manual switchover, as described in the “Performing a Manual Switchover” section on page 3-80.
- Step 8** Once the manual switchover is complete, log in to the newly active Cisco MGC, start an MML session and enter the following command to synchronize the Cisco MGCs:
- ```
prov-sync
```
- Step 9** Once the synchronization is complete, perform a manual switchover, as described in the “Performing a Manual Switchover” section on page 3-80.
- Step 10** Once the manual switchover is complete, log in to your newly standby Cisco MGC and change directories to the /opt/CiscoMGC/etc directory using the following UNIX command:
- ```
cd /opt/CiscoMGC/etc
```
- Step 11** Open the XECfgParm.dat file in a text editor, such as vi.
- Step 12** Search for the pom.dataSync property and ensure that it is set to *true*.
- Step 13** Save the file and exit the text editor.
- Step 14** Shut down the Cisco MGC software on your standby Cisco MGC, as described in the “Shutting Down the Cisco MGC Software Manually” section on page 2-4.
- Step 15** Start the Cisco MGC software on your standby Cisco MGC, as described in the “Starting the Cisco MGC Software” section on page 2-2.
-

## Rebooting Software to Modify Configuration Parameters

Sometimes you may need to change your configuration settings in the XECfgParm.dat file while the system is in-service. To do this, perform the following procedure:

**Caution**

Performing this procedure stops the functioning of the Cisco MGC software. Perform this step only while in contact with Cisco Technical Assistance Center (TAC) personnel. Refer to the “Obtaining Technical Assistance” section on page xviii for information on contacting the Cisco TAC.

- 
- Step 1** Log in to the active Cisco MGC and change directories to the etc subdirectory by entering the following UNIX command:
- ```
cd /opt/CiscoMGC/etc
```
- Step 2** Open the XECfgParm.dat using a text editor, such as vi.
- Step 3** Search for the parameters specified in the referring procedure and verify that it is set to the correct value. If they are set correctly, proceed to Step 10. Otherwise, proceed to Step 4 to begin the process of correcting your configuration.
- Step 4** Stop the Cisco MGC software on your active Cisco MGC, as described in the “Shutting Down the Cisco MGC Software Manually” section on page 2-4.
- Step 5** Modify the incorrect parameters identified in Step 3 to match their correct values.
- Step 6** Save your changes and close the text editor.
- Step 7** Restart the Cisco MGC software on your active Cisco MGC, as described in the “Starting up the Cisco MGC software manually” section on page 2-2.
- Step 8** Perform a manual switchover from the newly active Cisco MGC, as described in the “Performing a Manual Switchover” section on page 3-80.
- Step 9** Repeat steps 2 through 8 for the newly active Cisco MGC.
- If that resolves the problem, the procedure is complete. Otherwise, proceed to Step 10.
- Step 10** Contact the Cisco TAC to further analyze the problem and determine a solution. For more information about contacting the Cisco TAC, refer to the “Obtaining Technical Assistance” section on page xviii.
-

Resolving a Failed Connection to a Peer

If you have lost connection to a peer component in your network, perform the following procedure to resolve the problem:

-
- Step 1** Verify that the path to the affected peer is out-of-service, as described in the “Verifying the Status of all Destinations” section on page 3-8.
- If the destination is in-service, or there is no destination associated with the peer, proceed to Step 2.
- If the destination associated with the peer is out-of-service, bring the destination back into service, as described in the “SS7 Destination is Out of Service” section on page 8-57.

**Note**

If the out-of-service destination is IP destination, perform the procedure described in “Media Gateway IP Destination/Link Out-of-Service” section on page 8-98.

If that resolves the problem, this procedure is complete. Otherwise, proceed to Step 2.

- Step 2** Trace the route to the peer by entering the following UNIX command on your active Cisco MGC:

```
traceroute ip_addr
```

Where *ip_addr* is the IP address of the affected peer.

The system responds with a listing of the peers that are passed through on route to the identified peer.

If the system response indicates that the identified peer was reached with no problems, proceed to Step 4.

If the system response indicates that you were unable to reach the identified peer, proceed to Step 3.

- Step 3** Log in to the peer identified in Step 2 and verify that the Ethernet interfaces for this peer are working correctly. Refer to the documentation for the peer for more information.

If the Ethernet interfaces are working properly, proceed to Step 4.

If the Ethernet interfaces are not working properly, replace the element that is not working properly. Refer to the documentation of the peer for more information. If that resolves the problem, the procedure is complete. Otherwise, proceed to Step 4.

- Step 4** Contact the Cisco TAC to further analyze the problem and determine a solution. For more information about contacting the Cisco TAC, refer to the “Obtaining Technical Assistance” section on page xviii.



Configuring Cisco MGC Report Files

This appendix contains descriptions of the Cisco Media Gateway Controller (MGC) log files and the associated procedures for setting up the data dumper that controls how files are handled for three of those log file types. You can use these log records to obtain statistical information about the calls processed by the system and network events, such as delays or service-affecting conditions.

Understanding Logging Files

A log message consists of several fields. Refer to the *Cisco Media Gateway Controller Software Release 7 Messages Reference Guide* for detailed information on specific fields and valid values in log files.

Table A-1 lists the log file types for the Cisco MGC software. The Cisco MGC creates these log files and stores them in the `/$BASEDIR/var/log` directory, unless otherwise noted.

Table A-1 Log File Types

| Log File Type | Active Name | Archived Name | Description |
|----------------------------|--------------|-----------------------------|--|
| System | platform.log | platform_yyyymmddhhmmss.log | Contains log messages of varying severity created by system |
| Command | mml.log | MML_yyyymmddhhmmss.log | Man-Machine Language (MML) command category log messages |
| Alarms | alm.csv | alm_yyyymmddhhmmss_seq#.csv | Alarm category log messages. Archived files are stored in the <code>\$BASEDIR/var/spool</code> directory. |
| Measurements | meas.csv | meas_yyyymmddhhmmss.csv | Measurement category log messages. Archived files are stored in the <code>\$BASEDIR/var/spool</code> directory. |
| Call detail records (CDRs) | cdr.bin | cdr_yyyymmddhhmmss_seq#.bin | CDRs rotated on a regular basis. Archived files are stored in the <code>\$BASEDIR/var/spool</code> directory. |
| | | | Note CDRs can be stored in .csv format, if the TLV converter is enabled. Refer to the <i>Cisco Media Gateway Controller Software Release 7 Installation and Configuration Guide</i> for information on configuring the TLV converter. |

**Note**

The time stamps used on the archived file names (*yyyymmddhhmmss*) are in local time.

Configuring the Data Dumper

The Cisco MGC software contains a function called the data dumper that controls the destinations for active and archived log files for CDRs, measurements, and alarms, and controls when the active files are archived. The data dumper runs automatically and works correctly with a default configuration.

However, you can customize the dumper settings by editing the `dmprSink.dat` file. Here is an example of the contents of the `dmprSink.dat` file:

```
"callDetail" bin "cdr" "../var/log" "../var/spool" 1000 0 15
"measReport" csv "meas" "../var/log" "../var/spool" 500 0 15
"almState" csv "alm" "../var/log" "../var/spool" 500 0 15
```

The contents of the file displays the log file setup data for each of these three log file types. There are eight fields for each log file type in the file. The last three fields in each line can be modified to administer log file creation for these three log file types.

**Caution**

Do *not* modify any of the first five fields in each line.

The first field in each line identifies the log file type, such as *callDetail* for the CDR log files. The second field in each line identifies the storage format used in the log files. The storage format is either *bin* for binary, or *csv* for comma-separated-value. The third field identifies the file name used to identify the file type, such as *meas* for system measurements. The fourth field identifies the directory in which the active log files are stored, and the fifth field identifies the directory in which the archived log files are stored.

Table A-2 describes the last three fields in each line, which you can be modify, depending on your needs.

**Note**


At least one of the last three fields in each line *must* be set to a value other than zero (0) for logging to function properly.

Table A-2 Dumper Sink Log File Parameters

| Field Number | Default Value | Description |
|--------------|---------------|---|
| 6 | 1000 | Defines the maximum number of records a file can contain before it is flushed or moved to the spool directory. If this value is set to 0, the number of records is unlimited. You can improve system performance by increasing the value of this field to a larger value, such as 50000. This results in fewer log files being generated during periods of high call volume.

Note In the case of CDRs, the value in this field refers to the maximum number of call detail blocks (CDBs), which make up CDRs. Multiple CDBs can be created for each call. For more information on individual CDBs, refer to the <i>Cisco Media Gateway Controller Release 7 Billing Interface Guide</i> . |
| 7 | 0 | Defines the maximum size of the log file in bytes before it is moved to the spool directory. If this value is set to 0, the size of the file is limited only by the disk space available. |
| 8 | 15 | Defines the maximum time, in minutes, the file is allowed to remain open, before it is flushed or moved to the spool directory. If there is no data in the file, it is not flushed when the time limit expires. If this value is set to 0, there is no time limit. |

To configure the dmprSink.dat file fields, use this procedure:

-
- Step 1** Log in to the active Cisco MGC and change to the /opt/CiscoMGC/etc directory by entering the following UNIX command:
- ```
cd /opt/CiscoMGC/etc
```
- Step 2** Use a text editor, such as vi, to open and edit the dmprSink.dat file fields you want to change.
- 
-  **Note** If you are going to use the BAMS to collect CDRs, proceed to the “Configuring the Data Dumper to Support BAMS” section on page A-5, for information on how to configure the data dumper to support BAMS.
- 
- Step 3** Save your changes and exit the text editor.
- Step 4** Change to the /opt/CiscoMGC/etc/active\_link directory by entering the following UNIX command:
- ```
cd /opt/CiscoMGC/etc/active_link/
```
- Step 5** Repeat steps 2 and 3 for the version of dmprSink.dat stored in this directory.
- Step 6** If your system uses a continuous service configuration (active and standby Cisco MGC hosts), perform steps 9, 10, and 11 to update the settings on the standby Cisco MGC and load the new dmprSink.dat settings.
- If your system uses a simplex configuration (a single Cisco MGC host), perform steps 7 and 8 to load the new dmprSink.dat settings.
- Step 7** Stop the Cisco MGC software using the procedure described in the “Shutting Down the Cisco MGC Software Manually” section on page 2-4.

**Caution**

Stopping the Cisco MGC software should only be performed while in contact with Cisco Technical Assistance Center (TAC) personnel. Refer to the “Obtaining Technical Assistance” section on page xviii for information on contacting the Cisco TAC.

- Step 8** Restart the Cisco MGC software using the procedure described in the “Starting up the Cisco MGC software manually” section on page 2-2. The procedure is complete.
- Step 9** Repeat steps 1 through 5 on your standby Cisco MGC.
- Step 10** Log on to the active Cisco MGC, start an MML session and perform a manual switchover as described in the “Performing a Manual Switchover” section on page 3-80.
- Step 11** Once the manual switchover is complete, repeat Step 10 on the newly active Cisco MGC. The procedure is complete.
-

Configuring the Data Dumper to Support BAMS

If your system is going to be using the Billing and Measurements Server (BAMS) to retrieve CDRs from the Cisco MGC, perform the following procedure to configure the data dumper to support the BAMS:

Step 1 Log into the active Cisco MGC and change to the /opt/CiscoMGC/etc directory by entering the following UNIX command:

```
cd /opt/CiscoMGC/etc
```

Step 2 Use a text editor, such as vi, to open the dmprSink.dat file.

Step 3 In the callDetail line of the file, find the following directory path:

```
"../var/spool"
```

Step 4 Modify that directory path to point to the /opt/CiscoMGC/var/bam directory, as shown below:

```
"../var/bam"
```

Step 5 Save your changes and exit the text editor.

Step 6 Change to the /opt/CiscoMGC/etc/active_link directory by entering the following UNIX command:

```
cd /opt/CiscoMGC/etc/active_link/
```

Step 7 Repeat steps 2 through 5 for the version of dmprSink.dat stored in this directory.

Step 8 If your system uses a continuous service configuration (active and standby Cisco MGC hosts), perform steps 11, 12, and 13 to update the settings on the standby Cisco MGC and load the new dmprSink.dat settings.

If your system uses a simplex configuration (a single Cisco MGC host), perform steps 9 and 10 to load the new dmprSink.dat settings.

Step 9 Stop the Cisco MGC software using the procedure described in the “Shutting Down the Cisco MGC Software Manually” section on page 2-4.

**Caution**

Stopping the Cisco MGC software should only be performed while in contact with Cisco Technical Assistance Center (TAC) personnel. Refer to the “Obtaining Technical Assistance” section on page xviii for information on contacting the Cisco TAC.

Step 10 Restart the Cisco MGC software using the procedure described in the “Starting up the Cisco MGC software manually” section on page 2-2. The procedure is complete.

Step 11 Repeat steps 1 through 7 on your standby Cisco MGC.

Step 12 Log on to the active Cisco MGC, start an MML session and perform a manual switchover as described in the “Performing a Manual Switchover” section on page 3-80.

Step 13 Once the manual switchover is complete, repeat Step 10 on the newly active Cisco MGC. The procedure is complete.

Understanding the Format of Log Files Archived Using Data Dumper

Three log file types are archived in the \$BASEDIR/var/spool directory using the data dumper: alarms, measurements, and CDRs. The archive files for alarms and measurements are stored as ASCII text files, and the format of these files is discussed in this section. CDRs are stored as binary files and are not discussed here. The elements of CDR files are discussed in the *Cisco Media Gateway Controller Software Release 7 Billing Interface Guide*.

Here is an example of the appearance of the content of an archived alarm file:

```
0,1012522984,761,1,0,"Failover daemon in INIT state","FOD-01","unknown"
0,1012522989,880,1,0,"Failover daemon in SLAVE state","FOD-01","unknown"
0,1012522991,893,1,1,"Warm Start Initiated","IOCM-01","IosChanMgr"
0,1012522992,932,0,0,"Excessive bit error ratio detected from frame alignment
signal","enif1","IosChanMgr"
0,1012522992,936,0,0,"Excessive bit error ratio detected from frame alignment
signal","enif2","IosChanMgr"
0,1012522992,939,0,0,"Reset Config Failed","dpc1","IosChanMgr"
0,1012522992,939,1,2,"Point Code Unavailable","dpc1","IosChanMgr"
0,1012522992,958,0,0,"Reset Config Failed","dpc2","IosChanMgr"
0,1012522992,958,1,2,"Point Code Unavailable","dpc2","IosChanMgr"
0,1012522992,975,0,0,"Reset Config Failed","dpc-11","IosChanMgr"
0,1012522992,975,1,2,"Point Code Unavailable","dpc-11","IosChanMgr"
0,1012522993,37,0,0,"Reset Config Failed","dpc-12","IosChanMgr"
0,1012522993,38,1,2,"Point Code Unavailable","dpc-12","IosChanMgr"
0,1012522993,83,0,0,"Reset Config Failed","dpc-13","IosChanMgr"
0,1012522993,83,1,2,"Point Code Unavailable","dpc-13","IosChanMgr"
0,1012522993,99,0,0,"Reset Config Failed","dpc-14","IosChanMgr"
0,1012522993,123,1,2,"Point Code Unavailable","dpc-14","IosChanMgr"
0,1012522993,139,0,0,"Reset Config Failed","dpc-15","IosChanMgr"
0,1012522993,139,1,2,"Point Code Unavailable","dpc-15","IosChanMgr"
0,1012522993,155,0,0,"Reset Config Failed","dpc-16","IosChanMgr"
0,1012522993,156,1,2,"Point Code Unavailable","dpc-16","IosChanMgr"
```

Each field is separated by a comma. The content of each field is described in Table A-3.

Table A-3 Archived Alarm File Fields

| Field Name | Data Type | Maximum Length | Comments |
|--------------------------|-----------|----------------|---|
| Release level | Integer | 3 | Format of records (should be set to 0) |
| Timestamp (seconds) | Integer | 10 | Indicates the time, in seconds, since the start of the UNIX internal timer, time of epoch. |
| Timestamp (milliseconds) | Integer | 5 | Indicates the time, in milliseconds, since the start of the UNIX internal timer, time of epoch. |
| State | Integer | 1 | Used for informational alarms, either 0 for reset or 1 for set. |
| Severity | Integer | 1 | Indicates the severity of the alarm, using four levels: <ul style="list-style-type: none"> • 0—Informational • 1—Minor • 2—Major • 3—Critical |

Table A-3 Archived Alarm File Fields (continued)

| Field Name | Data Type | Maximum Length | Comments |
|----------------|-----------|----------------|--|
| Alarm category | String | 80 | Text that describes the nature of the alarm. For a list and description of the available alarms, refer to the <i>Cisco Media Gateway Controller Software Release 7 System Messages Guide</i> . |
| Component name | String | 32 | Identifies the component associated with the alarm. Refer to the <i>Cisco Media Gateway Controller Software Release 7 Provisioning Guide</i> for more information on components. |
| Originator | String | 32 | Identifies the service that set or cleared this alarm. |

Here is an example of the appearance of the content of an archived measurement file:

```
0,1012013100,900,0,"messages","SP: cInit out","ss7svc11"
0,1012013100,900,0,"occurrences","ACC: CALL REJ","hcss3-118"
0,1012013100,900,0,"occurrences","ACC: CALL REJ","hcss3-119"
0,1012013100,900,0,"messages","SP: cInit out","ss7svc5"
0,1012013100,900,0,"messages","SP: cInit out","ss7svc8"
0,1012013100,900,0,"messages","SP: cInit out","ss7svc9"
0,1012013100,900,0,"messages","SP: cInit out","ss7svc10"
0,1012013100,900,0,"occurrences","ACC: CALL REJ","hcss4-2"
0,1012013100,900,0,"occurrences","ACC: CALL REJ","tg-4166"
0,1012013100,900,0,"occurrences","ACC: CALL REJ","hcss4-3"
0,1012013100,900,0,"occurrences","ACC: CALL REJ","tg-4165"
0,1012013100,900,0,"occurrences","ACC: CALL REJ","hcss4-4"
0,1012013100,900,0,"occurrences","ACC: CALL REJ","hcss4-5"
0,1012013100,900,0,"occurrences","ACC: CALL REJ","tg-4164"
0,1012013100,900,0,"occurrences","ACC: CALL REJ","tg-4162"
0,1012013100,900,0,"occurrences","ACC: CALL REJ","hcss4-6"
0,1012013100,900,0,"occurrences","ACC: CALL REJ","tg-4163"
0,1012013100,900,0,"occurrences","ACC: CALL REJ","hcss4-7"
0,1012013100,900,0,"occurrences","ACC: CALL REJ","hcss4-8"
0,1012013100,900,0,"occurrences","ACC: CALL REJ","hcss4-9"
0,1012013100,900,0,"occurrences","ACC: CALL REJ","hcss4-10"
0,1012013100,900,0,"occurrences","ACC: CALL REJ","hcss4-11"
0,1012013100,300,0,"occurrences","ISUP: CHAN MATE UNAVAILABLE","ss7svc4"
```

Each field is separated by a comma. The content of each field is described in Table A-4.

Table A-4 Archived Measurement File Fields

| Field Name | Data Type | Maximum Length | Comments |
|-------------------------|-----------|----------------|--|
| Release level | Integer | 3 | Format of records (should be set to 0). |
| Timestamp (seconds) | Integer | 10 | Indicates the time, in seconds, since the start of the UNIX internal timer, time of epoch. |
| Time interval (seconds) | Integer | 5 | Duration of the collection interval. |
| Measurement value | Integer | 10 | Value of the measurement. |
| Measurement units | String | 32 | Units for which the measurement is recorded. |

Table A-4 Archived Measurement File Fields (continued)

| Field Name | Data Type | Maximum Length | Comments |
|----------------------|-----------|----------------|--|
| Measurement category | String | 32 | Text that describes the nature of the measurement. For a list and description of the available measurement, refer to Appendix D, “Cisco Media Gateway Controller Measurements.” |
| Component name | String | 32 | Identifies the component associated with the alarm. Refer to the <i>Cisco Media Gateway Controller Software Release 7 Provisioning Guide</i> for more information on components. |

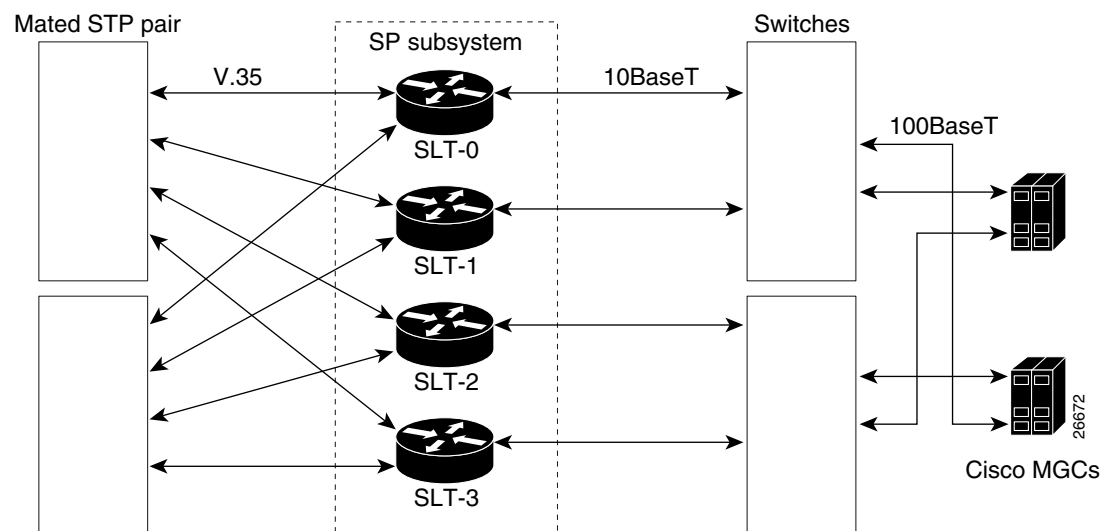


Troubleshooting Cisco SLT Signaling

Several Cisco 2600 series modular access routers can be utilized as hardware components called Cisco Signaling Link Terminals (SLTs). Cisco SLTs function as signaling link interfaces to SS7 Signal Transfer Point (STP) mated pairs on the SS7 network side. On the LAN side, Cisco SLTs function as IP interfaces to the Cisco Media Gateway Controllers (MGCs). A number of different SS7 messages pass between the Cisco SLTs and STPs and between the Cisco SLTs and Cisco MGCs through Cisco Catalyst Multiswitch Routers (MSRs), which are used as LAN switches.

Each STP in a mated pair is constantly active under normal operating conditions. SS7 message traffic normally flows between both STPs of the mated pair and the Cisco SLTs, as shown in Figure B-1.

Figure B-1 Cisco SLT Hardware and I/O Signaling



This chapter includes the following sections:

- Cisco SLT Signaling Overview, page B-2
- Troubleshooting SS7 Link Problems, page B-4
- Troubleshooting Cisco SLT-to-STP Signaling Links, page B-10
- Troubleshooting Cisco SLT to Cisco MGC Communications, page B-13
- Cisco SLT Error Messages, page B-15.

Cisco SLT Signaling Overview

This section contains the following subsections:

- IP Signaling Backhaul, page B-2
- Connection Management, page B-3

IP Signaling Backhaul

IP signaling backhaul is accomplished by means of the Cisco-proprietary Reliable User Datagram Protocol (RUDP) for communication between the Cisco SLT and the Cisco MGC.

Backhaul messages can be traced from the Cisco SLT command line interface (CLI) by means of the command

```
debug ss7 mtp2 backhaul channel
```

IP signaling backhaul is described in the following sections:

- Types of Encapsulation, page B-2
- PDU Verb Types, page B-2
- Backhaul Message IDs, page B-2

Types of Encapsulation

There are two different types of data encapsulation associated with IP signaling backhaul messages:

- Non-PDU messages—Defined as session manager control messages. These are used to control active and standby sessions with the respective Cisco MGCs.
- PDU messages—Messages the Session Manager delivers to the Message Transfer Part (MTP) Level 2 (MTP2). These messages are used to control MTP2 and to send and receive MSU messages.

PDU Verb Types

There are three different PDU verb types associated with IP signaling backhaul commands and messages:

- Requests—Messages sent only from the Cisco MGC to the Cisco SLT requesting that the Cisco SLT take some action, such as connect the link (align link), disconnect the link, or return its statistics.
- Confirmations—Messages sent from the Cisco SLT to the Cisco MGC in response to requests indicating that the requested action has been completed with success or failure.
- Indications—Asynchronous messages sent from the Cisco SLT to the Cisco MGC, indicating that the Cisco SLT has detected a state change, such as link alignment lost.

Backhaul Message IDs

There are five types of IP signaling backhaul message IDs:

- Backhaul reset commands
- Connection management commands
- Backhaul statistics messages

- Flow control
- Link status

Backhaul Reset

There are two types of IP signaling backhaul reset commands:

- **SoftReset (Link reset)**—Command is sent from the Cisco MGC to the Cisco SLT to put the backhaul signaling link in the Out-Of-Service (OOS) state. If the command succeeds, there is no response from the Cisco SLT because the backhaul link is out of service.

Sample message trace: 00:10:18: SoftResetRequest

- **HardReset (CPU reset)**—Command is sent from the Cisco MGC to the Cisco SLT to cause a CPU reset on the Cisco SLT.

Sample message trace: 00:10:18: HardResetRequest

Connection Management

There are two IP signaling backhaul connection commands; a connection request and a disconnect request. Each command has a corresponding confirmation message.

- **Connection request**—Command sent from the Cisco MGC to the Cisco SLT to request link alignment. The request indicates if the alignment is in a normal or emergency state.
- **Connection confirmation**—Reply sent from the Cisco SLT to the Cisco MGC in response to a connection request command to indicate its success or failure.

Sample message trace: 4d10h: MTP2: rcvd Conn Req - Emergency ch=0 Statistics—

- **Disconnect request**—Command sent from the Cisco MGC to the Cisco SLT to request that an In-Service (IS) link be taken OOS. The request is always processed.

The Cisco SLT transmits a status indicator, an Out-of-Service (SIOS) message on the SS7 link.

- **Disconnect confirmation**—Reply sent from the Cisco SLT to the Cisco MGC in response to a disconnect request command to indicate its success or failure.
- **Disconnect indication**—An asynchronous message sent from the Cisco SLT to the Cisco MGC, indicating that the Cisco SLT has detected a state change that calls for a disconnect request command, such as link alignment lost.

Sample message trace: 4d10h: MTP2: send Disc Ind ch=0 reason=0x7-LSSU condition

The following sections describe connections management:

- Backhaul Statistics, page B-3
- Backhaul Congestion, page B-4
- Link Status, page B-4

Backhaul Statistics

There are two IP signaling backhaul statistics messages:

- **Stats request**—Command sent from the Cisco MGC to the Cisco SLT to request that the Cisco SLT return its MTP Level 1 (MTP1) and MTP2 statistics. The request is always processed.

An action value is provided to accomplish one of three options: (1) return the statistics and reset the statistics collection, (2) just return the statistics, or (3) just reset the statistics collection.

- Stats confirmation—Reply sent from the Cisco SLT to the Cisco MGC in response to the stats request command.

Sample message trace: 4d10h: MTP2: rcvd Statistics Req-Send&Reset ch=0

Backhaul Congestion

The Cisco SLT uses the congestion indication, an asynchronous message sent from the Cisco SLT to the Cisco MGC to indicate that its backhaul signaling link is entering (Onset) or exiting (Abate) congestion.

Sample message trace:

```
Mar 1 005616.707 MTP2 send Flow Ind ch=0 status=0x0 start congestion
```

The Cisco SLT has two types of possible congestion. Both are determined in the same manner, but control flow in different directions.

- MTP2 signaling congestion—SS7 congestion deals with each individual SS7 link.
- Backhaul congestion—Deals with the active Session Manager session.

Congestion onset and abatement are determined by the percentage of free receive buffers.

- Congestion onset—An indication that the signaling node is congested.

When the number of free receive buffers drops below 20 percent, a backhaul congestion onset message is sent from the Cisco SLT to the Cisco MGC. At this point, the Cisco MGC holds all backhaul traffic destined for the Cisco SLT.

- Congestion abate—An indication that congestion has cleared.

When the number of free receive buffers rises above 40 percent, a backhaul congestion abate message is sent from the Cisco SLT to the Cisco MGC. At this point, the Cisco MGC resumes sending backhaul traffic destined for the Cisco SLT.

Link Status

Congestion status is maintained for backhaul.

Example of a congestion status message:

```
Nomad-C#sho ss7 mtp2 state
SS7 MTP2 states for channel 0
Protocol version for channel 0 is Bellcore GR-246-Core Issue 2, Dec 1997
MTP2LSC_INSERVICE      MTP2IAC_IDLE
MTP2TXC_INSERVICE      MTP2RC_INSERVICE
MTP2SUERM_MONITORING    MTP2AERM_IDLE
MTP2CONGESTION_IDLE
Congestion Backhaul     = Abate
Remote Processor Outage = FALSE
```

Troubleshooting SS7 Link Problems

The following sections describe methods of troubleshooting SS7 link problems:

- Checking Link Configuration Files, page B-5

- Checking UDP Traffic Flows, page B-5
- Checking Connection between Cisco MGC and Cisco SLT, page B-6
- Checking the T1/E1 Link State, page B-6
- Verifying the Link Alignment Status, page B-6
- Verifying Exchanged Point Codes, page B-7
- Cross-Checking Configuration Files, page B-8

Checking Link Configuration Files

Check the configuration files on the Cisco MGC and the Cisco SLT. The IP addresses and UDP ports must match.

- MTP2 Configuration:
 - Is the channel configured to the proper MTP2 variant?
 - Do the MTP2 variant protocol parameters match the remote configuration?
- Session Manager Configuration:
 - Are the proper number of sessions defined, session-0 and session-1?
 - Do the session configurations match the Cisco MGC session configurations?
 - Do the RUDP parameters match the Cisco MGC RUDP configuration?

Checking UDP Traffic Flows

Check UDP traffic flows between the Cisco MGC and the Cisco SLT by entering the following commands:

```
log on 2600, enable
debug ip udp
```

The response should look like the following, again depending on your configuration:

```
2600-1#deb ip udp
UDP packet debugging is on
2600-1#
15:06:53: UDP: rcvd src=10.15.13.6(7000), dst=10.15.13.2(7000), length=32
15:06:53: UDP: rcvd src=10.15.13.6(7000), dst=10.15.13.2(7000), length=32
15:06:53: UDP: sent src=10.15.13.2(7000), dst=10.15.13.6(7000), length=164
15:06:53: UDP: sent src=10.15.13.2(7000), dst=10.15.13.6(7000), length=164
15:06:53: UDP: rcvd src=10.15.13.6(7000), dst=10.15.13.2(7000), length=12
15:06:55: UDP: sent src=10.15.13.2(7000), dst=10.15.13.6(7000), length=32
15:06:55: UDP: rcvd src=10.15.13.6(7000), dst=10.15.13.2(7000), length=12
un all
```

Check for traffic in both directions. If there is traffic, go to the “Checking Connection between Cisco MGC and Cisco SLT” section on page B-6.

Otherwise, verify IP addresses, try to ping in both directions, reload the Cisco SLT software, check subnets, and check the VLANs on the LAN switches.

Checking Connection between Cisco MGC and Cisco SLT

Check that the Cisco MGC connects to the Cisco SLT:

```
debug ss7 mtp2 backhaul ip upd N
```

Where $N = 0, 1, 2$, or 3 , which identifies the specific MTP link.

The Cisco SLT will not attempt to align the link until it has received an MTP3 Connect Indication from the Cisco MGC. The MTP3 primitives between the Cisco SLT and the Cisco MGC can be seen with this debug command.

Checking the T1/E1 Link State

Check the T1 or E1 link state by observing the LEDs on the Cisco SLT. Make sure that the framing options match on both sides of the physical link.

Verifying the Link Alignment Status

Check alignment status of a link by entering the following debug command:

```
debug ss7 mtp2 iac N
```

Where N is a number ($0, 1, 2$, or 3) that identifies the specific MTP link.

Table B-1 describes various debug outputs from the previous command, the probable cause, and the recommended recovery. This traffic is exchanged only when the link is initially brought up. If the link is already In-Service, nothing is displayed.

Table B-1 Debug Outputs, Probable Causes, and Recovery Actions

| Debug Output | Probable Cause | Recovery Action |
|--------------|--|--|
| No output. | Link is already aligned.
MTP2 is not started. | 1. Check that term monitor is on.
2. Reload Cisco SLT.
3. Cross-check configuration files. |

Table B-1 Debug Outputs, Probable Causes, and Recovery Actions

| Debug Output | Probable Cause | Recovery Action |
|---|--|---|
| <pre>2600-1#deb ss7 mtp2 iac 0 2600-1# 15:12:33: itu2IAC_Start chnl=0 MTP2IAC_IDLE 15:12:34: itu2IAC_Stop chnl=0 MTP2IAC_NOT_ALIGNED 15:12:39: itu2IAC_Start chnl=0 MTP2IAC_IDLE 15:12:51: itu2IAC_T2_TMO chnl=0 MTP2IAC_NOT_ALIGNED 15:12:56: itu2IAC_Start chnl=0 MTP2IAC_IDLE 15:13:07: itu2IAC_T2_TMO chnl=0 MTP2IAC_NOT_ALIGNED 15:13:12: itu2IAC_Start chnl=0 MTP2IAC_IDLE</pre> | <p>MTP2 does not flow across the link.</p> | <p>Check DS0 assignment (should use the same time slot on both sides of the physical link) and the DS0 speed (defaults to 56 kbps on T1 and 64 kbps on E1). The DS0 speed can be changed by</p> <pre>conf t contr E1 0/0 channel-group 0 timeslot 1 speed 56</pre> |
| <pre>2600-1#deb ss7 mtp2 iac 0 2600-1# 15:14:32: itu2IAC_Start chnl=0 MTP2IAC_IDLE 15:14:33: itu2IAC_Rcvd_SIE chnl=0 MTP2IAC_NOT_ALIGNED 15:14:33: itu2IAC_Rcvd_SIE chnl=0 MTP2IAC_ALIGNED 15:14:37: itu2IAC_T4_TMO chnl=0 MTP2IAC_PROVING 15:14:38: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0:0, changed state to up 15:14:45: itu2IAC_Rcvd_SIOS chnl=0 MTP2IAC_IDLE 15:14:46: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0:0, changed state to down 15:14:50: itu2IAC_Start chnl=0 MTP2IAC_IDLE 15:14:50: itu2IAC_Rcvd_SIE chnl=0 MTP2IAC_NOT_ALIGNED 15:14:50: itu2IAC_Rcvd_SIE chnl=0 MTP2IAC_ALIGNED 15:14:54: itu2IAC_T4_TMO chnl=0 MTP2IAC_PROVING 15:14:55: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0:0, changed state to up</pre> | <p>The link is able to align, but fails in the PROVING sequence.</p> <p>It is generally a mismatch in point codes.</p> | <p>Check the provisioning settings for the SLC, OPC, and DPC in the Cisco MGC, as described in the “Bouncing SS7 Links” section on page 8-56.</p> <p>You can use an SS7 sniffer tool to look at the exchanged point codes. The procedure in “Verifying Exchanged Point Codes” section on page B-7 allows you to get them using Cisco SLT debug tools.</p> |

Verifying Exchanged Point Codes

Check exchanged point codes by entering the following command:

```
debug ss7 mtp2 pac N
```

Where: $N = 0, 1, 2$, or 3 identifies the MTP link

Table B-2 describes various debug outputs from this command, the probable cause, and the recommended recovery.

Table B-2 Debug Outputs, Probable Causes, and Recovery Actions

| Debug Output | Probable Cause | Recovery Action |
|---|---|---|
| No output | MTP2 is not started. | <ol style="list-style-type: none"> 1. Check that term monitor is on. 2. Reload the Cisco SLT. 3. Cross check configuration files. |
| <pre> 2600-1#deb ss7 mtp2 pac 0 2600-1# 15:08:31: MTP2 incoming trace enabled on channel 0. 15:08:31: MTP2 outgoing trace enabled on channel 0. 15:08:34: ---- Outgoing Rudp msg (41 bytes) ---- SM_msg_type 0x00008000 protocol_type 0x0001 msg_ID 0x0000 msg_type 0x0011 channel_ID 0x0000 bearer_ID 0x0000 length 0x0019 data 0xB2236ED6 0x006FD600 0x11F01122 0x33445566 0x778899AA 0xBBCCDDEE 15:08:34: ---- Incoming Rudp msg (41 bytes) ---- SM_msg_type 0x00008000 protocol_type 0x0001 msg_ID 0x0000 msg_type 0x0010 channel_ID 0x0000 bearer_ID 0x0000 length 0x0019 data 0xB2006FD6 0x236ED600 0x21F01122 0x33445566 0x778899AA 0xBBCCDDEE unall </pre> | <p>Cisco MGC is exchanging messages with remote SP.</p> <p>Exchanged point codes must match before communication can be successfully established.</p> | <p>Check point codes: in data 0xB2236ED6 0x006FD6:</p> <ol style="list-style-type: none"> 1. 236ED6 should be read D6-6E-23 and converted in decimal: 214-110-035, which is the point code of the MGC. 2. 006FD6 should be read D6-6F-00 and converted in decimal: 214-111-000, which is the point code of the STP in this example. <p>The values in the incoming and outgoing messages must match.</p> |

Cross-Checking Configuration Files

Cross-check the configuration files by entering the following command:

```
2600-1#deb ss7 mtp2 iac 0
```

You should see a response similar to the following Cisco MGC sample configuration file:

File: XECfgParm.dat (extract)

```

*.ipAddrLocalA = 10.15.13.6 # Should be same as *.IP_Addr1
*.ipAddrLocalB = 10.15.13.22
*.ipAddrPeerA = 0.0.0.0 # Failover peer's address
*.ipAddrPeerB = 0.0.0.0

*.IP_Addr1 = 10.15.13.6 # Address of interface on motherboard
*.IP_Addr2 = 10.15.13.22
*.IP_Addr3 = 0.0.0.0
*.IP_Addr4 = 0.0.0.0
*.stPort = 0

```

This file defines the Cisco MGC IP addresses used to communicate with the Cisco SLT.

To check if they match with the Solaris configuration, you can use **ifconfig** -a Solaris command.

```
File: sigChanDev.dat
001d0001 0 1 00080002 00030014 00060001 0
001d0002 0 1 00080001 00030014 00060001 1
001d0003 1 1 00080001 00030014 00060002 1
001d0004 1 1 00080002 00030014 00060002 0
001d0005 2 1 00080002 00030014 00060001 0
001d0006 2 1 00080001 00030014 00060001 1
001d0007 3 1 00080001 00030014 00060002 1
001d0008 3 1 00080002 00030014 00060002 0
```



Note

The last digit in each line (0 or 1 in this example) identifies the link ID on the Cisco SLT. It can take the value 0, 1, 2, or 3 and is misleadingly identified as a timeslot in Cisco MGC provisioning. Only two STP links can be used on the Cisco SLT.

```
File: sigChanDevIp.dat

001d0001 IP_Addr1 7000 10.15.13.2 7000
001d0002 IP_Addr1 7000 10.15.13.2 7000
001d0003 IP_Addr2 7000 10.15.13.19 7000
001d0004 IP_Addr2 7000 10.15.13.19 7000
001d0005 IP_Addr1 7000 10.15.13.4 7000
001d0006 IP_Addr1 7000 10.15.13.4 7000
001d0007 IP_Addr2 7000 10.15.13.21 7000
001d0008 IP_Addr2 7000 10.15.13.21 7000
```

This file associates the Cisco MGC IP address/UDP port to the Cisco SLT IP address/UDP port. IP_Addr1 and IP_Addr2 are defined in XECfgParm.dat.

These files should not be edited using vi. Any change is lost when provisioning tools are used. The only exception is XECfgParm.dat (and changes can be lost anyway).

Cisco SLT sample configuration:

```
controller T1 0/0
framing esf
linecode b8zs
channel-group 0 timeslots 1
!
controller T1 0/1
framing esf
linecode b8zs
channel-group 0 timeslots 1
!
interface Ethernet0/0
ip address 10.15.13.2 255.255.255.240
no ip directed-broadcast
!
interface Serial0/0:0
no ip address
no ip directed-broadcast
!
interface Ethernet0/1
ip address 10.15.13.18 255.255.255.240
no ip directed-broadcast
!
interface Serial0/1:0
no ip address
no ip directed-broadcast
!
```

```

ip classless
ip route 172.18.0.0 255.255.0.0 10.15.13.1
no ip http server
!
ss7 set failover-timer 3
ss7 session-0 address 10.15.13.6 7000 10.15.13.2 7000
ss7 session-0 retrans_t 600
ss7 session-0 cumack_t 300
ss7 session-0 kp_t 2000
ss7 session-0 m_retrans 2
ss7 session-0 m_cumack 3
ss7 session-0 m_outseq 3
ss7 session-0 m_rcvnum 32
!
line con 0
transport input none
line aux 0
line vty 0 4
login
!
end

```

Troubleshooting Cisco SLT-to-STP Signaling Links

Cisco SLTs interface with STPs through linksets. STP linksets can support a maximum of 16 individual SS7 signaling links. Each Cisco SLT can be configured to interface with as many as two individual SS7 signaling links. Cisco SLTs support SS7 Message Transfer Part Levels 1 and 2 (MTP1 and MTP2) in the Cisco SLT-to-STP signaling link interfaces.

When a Cisco SLT is replaced with a new unit, complete the following steps to determine whether the original Cisco SLT was the cause of the SS7 communication problem:

-
- Step 1** Connect an SS7 protocol analyzer to a patch panel monitor port to monitor the SS7 message traffic entering or leaving the Cisco SLT-to-STP link.
 - Step 2** Monitor the SS7 message traffic (if any) between the STP and the Cisco SLT.
 - Step 3** If SS7 traffic is being received from the STP, continue with the next step.
If no SS7 message traffic is being received, go to the “MTP1 Communication Problems” section on page B-11.
 - Step 4** Ensure that SS7 Message Signaling Units (MSUs), Fill-in Signaling Units (FISUs), or Link Status Signaling Units (LSSUs) are being transceived by the Cisco SLT.
 - Step 5** If SS7 LSSU messages are being transceived, go to the “MTP2 Communication Problems” section on page B-12.
If SS7 LSSU messages are not being transceived, go to the next step.
 - Step 6** If SS7 MSU and FISU messages are being transceived by the Cisco SLT go to the “Troubleshooting Cisco SLT to Cisco MGC Communications” section on page B-13.
 - Step 7** If SS7 MSU and FISU messages are not being transceived, replace the faulty Cisco SLT with a backup unit, if one is available.

If the problem is no longer present with the replacement unit, you can test the faulty unit offline to determine the cause of the problem.
-

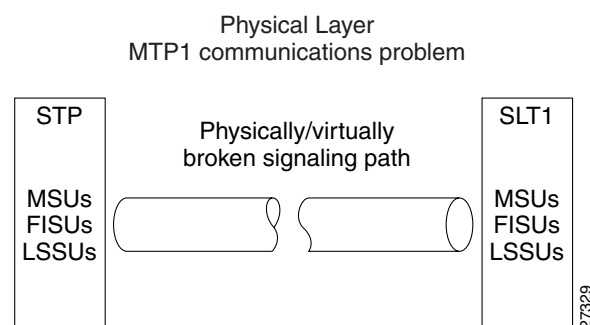
MTP1 Communication Problems

The next two sections describe the procedures for identifying and solving MTP1 communication problems. The initial indication of signaling problems may change in T1 (or E1) status. Check for alarms on the T1 (or E1) interface before performing any of the following procedures.

Identifying MTP1 Communication Problems

MTP1 standardizes SS7 signaling link physical connectivity. When an MTP1 problem occurs, there is a physical connection break or a virtual break (something that causes the symptoms of a physical connection break, such as no power to a card slot) in the signaling link path. A break is identified when no Message Signaling Unit (MSU), Fill-In Signaling Unit (FISU), or Link Status Signaling Unit (LSSU) traffic can be sent or received over the SS7 link. MTP1 communication problems are normally the result of either a hardware failure, a cabling problem, or a physical interface problem.

Figure B-2 Physical Layer, MTP1 Communication Problems



Resolving MTP1 Communication Problems

If monitoring the SS7 link with a protocol analyzer reveals no MSU, FISU, or LSSU message traffic, complete the following steps:

-
- Step 1** Ensure that power is on to the Cisco SLT.
 - Step 2** Check to ensure that the STP signal link cabling is correctly connected to the Cisco SLT.
 - Step 3** Disconnect the Cisco SLT from both the STP and the LAN switch for offline testing. Connect two recommended SS7 protocol analyzers, one to the STP interface the other to the IP interface.

One SS7 protocol analyzer must be equipped to send/receive SS7 test messages to the Cisco SLT over the V.35 interface, and the other to send/receive messages to the Cisco SLT over the IP interface.



Caution

Do not leave the Cisco SLT connected to the LAN switch, and thus the Cisco MGC, while injecting SS7 test messages into the Cisco SLT. The Cisco MGC might not properly recognize the SS7 test messages generated by your protocol analyzer, which could cause error conditions between the Cisco MGC and the Cisco Media Gateway.

- Step 4** Test Cisco SLT ports and hardware by conducting a loop test of the signal link, excluding connectivity to the distant end SS7 node and the LAN switch.

- Step 5** If no MTP1 problem is discovered by the test, then the MTP1 problem more than likely resides within the STP node or the connection to the STP node. If the problem is within the Cisco SLT, replace the unit.

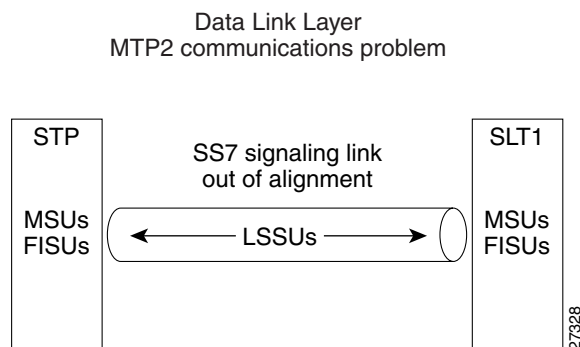
MTP2 Communication Problems

The next two sections describe the procedures for identifying and solving MTP2 communication problems.

Identifying MTP2 Communication Problems

MTP2 standardizes SS7 signaling link alignment. MTP2 communication problems occur when Cisco SLTs cannot establish data link alignment with STPs. When this happens the FISUs and MSUs cease to be transmitted. FISUs and MSUs are replaced by LSSUs whenever an SS7 link has good physical connectivity (MTP1), but cannot align to send and receive either FISU or MSU traffic.

Figure B-3 Data Link Layer, MTP2 Communication Problem



Resolving MTP2 Communication Problems

If monitoring of the SS7 link with a protocol analyzer reveals no MSU or FISU message traffic (only LSSU traffic), complete the following steps:

- Step 1** Check to ensure that the signal link cabling is correctly connected to the Cisco SLT.
- Step 2** Disconnect the Cisco SLT from both the STP and the LAN switch for offline testing. Connect two recommended SS7 protocol analyzers.
- One SS7 protocol analyzer must be equipped to send/receive SS7 test messages to the Cisco SLT over the V.35 interface, and the other to send/receive messages to the Cisco SLT over the IP interface.
- Step 3** Test router ports and hardware by conducting a loop test of the signal link, excluding connectivity to the distant end SS7 node.
- Step 4** If no MTP2 (link alignment) problem is discovered by the test, then the problem more than likely resides within the distant end STP node.
- If a problem is discovered with the Cisco SLT, replace the unit.

Troubleshooting Cisco SLT to Cisco MGC Communications

Cisco SLTs communicate with Cisco MGCs through a Cisco Catalyst MSR used as a LAN switch. Under normal conditions all Cisco SLTs actively process SS7 message traffic from the STPs. However, only one of the two Cisco MGCs actively processes traffic at any one time. One Cisco MGC always stays in a hot-standby mode while the other actively processes message traffic.

Routing, call control, network management, and all other SS7 application data is framed within SS7 protocol layers MTP3 and higher. The Cisco SLTs, which support MTP1 and MTP2 functionality, pass MTP3 and higher-layer SS7 protocol data between the Cisco MGCs and STP mated pairs.

Cisco SLT to Cisco MGC communication comprises multiple Cisco SLTs, which pass SS7 message traffic on to the Cisco MGCs through the LAN switches. Each STP linkset coming into a Cisco SLT normally has links connected to at least two Cisco SLTs to ensure network survivability.

The Cisco-proprietary Reliable User Datagram Protocol (RUDP) is used for Cisco SLT to Cisco MGC communication. In a fault-tolerant configuration, for example, Ethernet 10BaseT links each Cisco SLT to two LAN switches, and 100BaseT links each LAN switch to both the active Cisco MGC and the standby Cisco MGC.

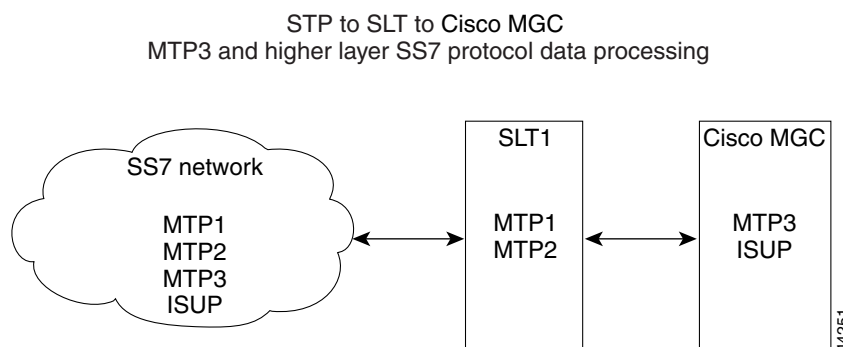
Identifying MTP3 and Higher Layer Problems

Although the Cisco SLTs normally pass MTP3 and higher-layer data directly to the Cisco MGCs, Cisco SLT hardware could also be the cause of MTP3 and higher layer SS7 communication problems. Cisco SLT-originated MTP3 or higher layer SS7 problems can affect message traffic over a certain link, or just the links that transceive through a certain Cisco SLT.

Cisco SLTs package received SS7 message data into RUDP datagrams that are transmitted through the LAN switches onto the Cisco MGC. This process is reversed (Cisco SLT strips RUDP datagrams) and standard SS7 message framing is added by the Cisco SLTs when the Cisco MGCs send SS7 messages to the Cisco SLTs.

If a tested SS7 link has connectivity (MTP1) and alignment (MTP2), but SS7 error messages are reported by network management tools, then there is probably an MTP3 or higher layer SS7 communication problem. This problem requires testing to verify Cisco SLT operation.

Figure B-4 MTP3 and Higher-Layer SS7 Protocol Processing



Resolving MTP3 and Higher Layer SS7 Communication Problems

Coordinate a signaling link test of the SS7 transceive path within the system, excluding connectivity to distant end SS7 nodes. Use a recommended SS7 protocol analyzer to send SS7 messages to the suspected Cisco SLT while monitoring the output of the Cisco SLT with a recommended protocol analyzer. If no MTP1 (connectivity), MTP2 (link alignment), or MTP3 or higher layer problem is discovered by the test, then the problem probably is not the Cisco SLT under test.



Caution

Do not leave the Cisco SLT connected to the LAN switch, and thus the Cisco MGC, while injecting SS7 test messages into the Cisco SLT. The Cisco MGC might not properly recognize the SS7 test messages generated by your protocol analyzer, which could cause error conditions between the Cisco MGC and the media gateway.

Identifying Ethernet Connectivity Problems

SS7 message components are Ethernet framed and transceived through one of the Cisco SLT's two Ethernet 10BaseT ports. A physical break or a virtual break will result in a percentage of message traffic not being received along the Cisco MGC path (Cisco SLT-to-LAN switch-to-Cisco MGC). Utilization of a Packet Internet Groper (PING) utility program to perform echo response tests should suffice to identify Ethernet connectivity problems within these components.

Identifying IP Communication Problems

Cisco SLT traffic is routed, rerouted, and, if necessary, retransmitted to the Cisco MGCs through the LAN switches. Monitoring for the following Internet Control Message Protocol (ICMP) error-reporting datagrams will assist in identifying IP communication problems:

- Destination Not Reachable/No Echo Reply
- Source Quench/Receiving Buffer Congestion
- Redirection Required
- Time to Live Exceeded
- Parameter Problems
- Timestamp Request/Reply
- Echo Request/Reply

If IP communication is good, then the RUDP application layer software could be the cause of the problem. Utilizing echo and timestamp request messages and monitoring response messages should be sufficient to identify RUDP/IP/Ethernet communication problems within the system.

Cisco SLT Error Messages

Table B-3 lists the Cisco SLT error messages broadcast by the Cisco MGC.

Table B-3 Cisco SLT Error Messages

| Message Name | Definition | Recommended Action |
|--|--|---|
| OWNERR, PQUICC, LOG_ERR, MSG_TRACEBACK MSG_PROCESS | An internal software error has occurred. | Call your technical support representative for a software upgrade for the Cisco SLT. |
| INITFAIL, PQUICC, LOG_ALERT, 0, "PQUICC(%d%d), SCC%d init failed" | The software failed to initialize/restart a 1T serial card. | Clear the serial interface. If the message recurs, call your technical support representative for assistance. |
| CTSLOST, PQUICC, LOG_ALERT, 0, "PQUICC(%d%d), Clear to Send Lost" | The Clear To Send (CTS) input signal on a data terminal equipment (DTE) serial interface became inactive while transmitting a frame. This is the result of a communication line failure or cable disconnection. | Check the serial interface cable and/or communication equipment, such as the channel service unit/data service unit (CSU/DSU). |
| UNDERFLO, PQUICC, LOG_ALERT, 0, "PQUICC(%d%d), Transmit Underflow" | While transmitting a frame, the serial controller chip's local buffer received insufficient data, because data could not be transferred to the chip fast enough to keep pace with its output rate. Normally, such a problem is temporary, depending on transient peak loads within the system. | The system should recover; no action is required. |
| LINEFLAP, PQUICC, LOG_ALERT, 0, "PQUICC(%d%d), Excessive modem control changes" | The system received too many modem control signal interrupts. Modem control signals are hardware handshake signals between data terminal equipment (DTE) and data communications equipment (DCE). The signals include either a data carrier detect (DCD) or a data set ready (DSR), or both. | Check the serial interface cable. The error can occur if the cable is disconnected or has come loose and is picking up noise. If the cable appears to be connected correctly, check the equipment connected to the cable." |
| BADHDXFSM, PQUICC, LOG_ALERT, 0, "PQUICC(%d%d), Unexpected HDX state %d, event %d" | A bad event was detected in the state machine for half duplex transmission/reception. | Copy the error message exactly as it appears, and report it to your Cisco technical support representative. |
| TOOSMALL, PQUICC, LOG_ALERT, 0, "PQUICC(%d/%d), packet was less than 2 bytes" | A small packet (less than 2 bytes) was queued up for transmission. The interface cannot handle such small packets for transmission. | The system should recover. No action is required. If the message recurs, it might indicate a hardware error related to data traffic patterns. Copy the error message exactly as it appears, and report it to your Cisco technical support representative. |

Table B-3 Cisco SLT Error Messages (continued)

| Message Name | Definition | Recommended Action |
|---|---|---|
| TOOBIG, PQUICC, LOG_ALERT, 0, "PQUICC(%d/%d), packet too big"; | A packet greater than the assigned MTU of this serial interface was queued up for transmission. | The system should recover. No action is required. If the message recurs, it might indicate an error related to data traffic patterns. Copy the error message exactly as it appears, and report it to your Cisco technical support representative. |
| UNKNOWN_WIC, PQUICC, LOG_ALERT, 0, "PQUICC(%d), WIC card has an unknown ID of 0x%x" | The software does not recognize the WAN Interface Card (WIC) plugged into the port module. | Check part number on the WIC card to verify it is supported in the Cisco IOS release operational on the router, or contact your Cisco technical support representative. |

If you need to contact your technical support representative for assistance, be prepared to provide the Cisco SLT and Cisco MGC debug trace information captured while the problem was occurring. In most cases, the backhaul trace and the LSC trace from the Cisco SLT would be required. If the problem is associated with link alignment, you should also include the IAC trace output. Trace information can help the investigator delineate the problem to the Cisco SLT or to the Cisco MGC.

To enable MTP2 traces, enter the following commands:

```
debug ss7 mtp2 back channel
debug ss7 mtp2 lsc channel
debug ss7 mtp2 iac channel
```

To turn debug trace off, enter the command **un all**

The output from a **show version** command provides explicit details about the image and branch info. This information tells specifically which branch of code to investigate.

The output from a **show run** command indicates what Cisco SLT configuration is in use. This is important because many problems can be caused by improper configurations, such as timer durations.

Provide any information from show commands that you used to identify the problem; for example:

```
show ss7 sm stats
```

Include any other information that might be useful in understanding or reproducing the problem. This information will help your technical support representative verify the fix.



Troubleshooting Cisco Catalyst 5500 Multiswitch Routers Signaling

Two Cisco Catalyst 5500 Multiswitch Routers (MSRs) are used in fault-tolerant Cisco telephony solutions. Both MSRs are active. Virtual local area networks (VLANs) are set up within these MSRs. The MSR VLANs are used by system components to route message traffic to other system components. The Catalyst 5500 is equipped with an interswitch link (ISL), which connects the active MSR to the standby MSR.

Normally, at least two Cisco Signaling Link Terminals (SLTs) are connected to each MSR for redundancy. SS7 call messages travel from the Cisco SLTs through the MSR VLANs and on to the Cisco Media Gateway Controllers (MGCs). MSR VLANs can also be used to link the Cisco MGCs to the Media Gateways (MGWs).

This chapter includes the following sections:

- MSR VLANs, page C-1
- Command Line Interface, page C-2
- Troubleshooting MSR Virtual Pathways and ISLs, page C-3

MSR VLANs

VLANs are configured within each MS, and help to simplify MSR management. All intrasystem-MSR Ethernet message traffic is partitioned and routed over VLANs according to component origination and destination. Route Switch Modules (RSM) within the MSRs control the routing of inter-VLAN message traffic. The active MSR VLAN configuration is exactly the same as that of the standby MSR VLANs.

For example, VLANs within the active MSR can provide paths to ports of the following components:

- VLAN 1 (black) provides a path to ports on modules one and two of the Supervisor Engine.
- VLAN 2 (green) provides a path to a port on each of the four Cisco SLTs and the two Cisco MGCs.
- VLAN 3 (blue) provides a path to ports on the Cisco Media Gateways (MGWs).
- VLAN 4 (red) provides a path to ports on each of the two Cisco MGCs.

Command Line Interface

Access to the Command Line Interface (CLI) can be gained either locally through a console terminal connected to an EIA/TIA-232 port or remotely through a Telnet session. Telnet session access requires a previously set IP address for the switch. Telnet sessions are automatically disconnected after remaining idle for a configurable time period.

There are two modes of operation—normal and privileged—both password protected. Normal-mode commands are used for everyday system monitoring. Privileged commands are used for system configuration and basic troubleshooting.

After you log in successfully, the system automatically enters normal mode, which gives you access to normal-mode commands only. You can enter privileged mode by entering the enable command followed by a second password. Privileged mode is indicated by the appearance of the word "enable" immediately after the system prompt. To return to normal mode, enter the disable command at the prompt.

Commands entered from the CLI can apply to the entire system or to a specific module, port, or virtual local area network (VLAN). Catalyst 5500 modules (module slots), ports, and VLANs are numbered starting with 1. The supervisor module is module 1, residing in the top slot. If you are using a Catalyst 5500 with a redundant supervisor engine, the supervisor modules reside in slots 1 and 2. On each module, port 1 is the leftmost port.

To reference a specific port on a specific module, the command syntax is `mod_num/port_num`. For example, `3/1` denotes module 3, port 1. In some commands, such as `set trunk`, `set cam`, and `set VLAN` commands, you can enter lists of ports and VLANs. Designate ports by entering the module and port number pairs, separated by commas. To specify a range of ports, use a dash (-) between the module number and port number pairs. Dashes take precedence over commas.

The following examples show several ways of designating ports:

Example 1: `2/1,2/3` denotes module 2, port 1 and module 2, port 3

Example 2: `2/1-12` denotes module 2, ports 1 through 12

Example 3: `2/1-2/12` is the same as Example 2

Each VLAN is designated by a single number. You specify lists of VLANs in the same way that you do for ports. Individual VLANs are separated by commas (;); ranges are separated by dashes (-). In the following example, VLAN numbers 1 through 10 and VLAN 1000 are specified:

```
1-10,1000
```

Some commands require a Media Access Control (MAC) address, IP address, or IP alias, which must be designated in a standard format. The MAC address format must be six hexadecimal numbers separated by hyphens, as shown in this example:

```
00-00-0c-24-d2-fe
```

The IP address format is 32 bits, written as four octets separated by periods (dotted decimal format) that are made up of a network section, an optional subnet section, and a host section, as shown in this example:

```
126.2.54.1
```

If the IP alias table is configured, you can use IP aliases in place of the dotted decimal IP address. This is true for most commands that use an IP address, except commands that define the IP address or IP alias. For more information about the `set interface` and `set IP alias` commands, refer to the *Catalyst 5000 Series Command Reference*.

Command Line Interface Local Access

To obtain local access to the CLI, complete the following steps:

-
- Step 1** At the Console> prompt, press **Return** (or **Enter**).
 - Step 2** At the Enter Password: prompt, enter the system password. The Console> prompt appears indicating that you have successfully accessed the CLI in normal operation mode.
 - Step 3** Enter the necessary commands to complete the required task.
 - Step 4** Enter **quit** and press **Return** (or **Enter**) to exit the session.
-

Command Line Interface Remote Access

To obtain remote access to the CLI, complete the following steps:

-
- Step 1** From the remote host, enter the Telnet command and designate the name or IP address of the switch you wish to access (Telnet hostname | IP address).
 - Step 2** At the Enter Password: prompt, enter the password for the CLI. There is no default password (just press **Return** or **Enter**) unless a password was previously established using the set password command.
 - Step 3** Enter the necessary commands to complete the required task.
 - Step 4** Enter quit and press **Return** (or **Enter**) to exit the Telnet session.
-

Troubleshooting MSR Virtual Pathways and ISLs

Use of a recommended protocol analyzer (locally or remotely) equipped with a recommended Packet Internet Groper (PING) utility program to perform Ethernet echo response tests should identify MSR hardware, VLAN, and ISL connectivity problems. Echo is used to detect if another host is active on the network. The sender initializes the identifier and sequence number (which is used if multiple echo requests are sent), adds some data to the data field, and sends the ICMP echo to the destination host. The ICMP header code field is zero. The recipient changes the type to Echo Reply and returns the datagram to the sender. This mechanism is used to determine if a destination host is reachable.

To use the PING command, complete the following steps:

-
- Step 1** Log in to the CLI and enter the command:

Console> **show port status**

A response, similar to the following, is displayed:

| Port | Name | Status | Vlan | Level | Duplex | Speed | Type |
|------|------|------------|-------|--------|--------|-------|--------------|
| 1/1 | | connected | 523 | normal | half | 100 | 100BaseTX |
| 1/2 | | notconnect | 1 | normal | half | 100 | 100BaseTX |
| 2/1 | | connected | trunk | normal | half | 400 | Route Switch |
| 3/1 | | notconnect | trunk | normal | full | 155 | OC3 MMF ATM |
| 5/1 | | notconnect | 1 | normal | half | 100 | FDDI |
| 5/2 | | notconnect | 1 | normal | half | 100 | FDDI |

Step 2 Enter the CLI command **Show VLAN**.

```
Console> (enable) show vlan 998
```

A response, similar to the following, is displayed:

| VLAN | Name | Status | IfIndex | Mod/Ports, Vlans |
|------|----------|--------|---------|------------------|
| 998 | VLAN0998 | active | 357 | |

| VLAN | Type | SAID | MTU | Parent | RingNo | BrdgNo | Stp | BrdgMode | Trans1 | Trans2 |
|------|-------|--------|------|--------|--------|--------|-----|----------|--------|--------|
| 998 | trcrf | 100998 | 4472 | 999 | 0xff | - | - | srb | 0 | 0 |

| VLAN | AREHops | STEHops | Backup | CRF |
|------|---------|---------|--------|-----|
| 998 | 10 | 10 | off | |

Step 3 Enter (for ISLs) the command **Show Trunk**.

```
Console> (enable) show trunk
```

A response, similar to the following, is displayed:

| Port | Mode | Encapsulation | Status | Native vlan |
|------|-----------|---------------|----------|-------------|
| 2/1 | desirable | dot1q | trunking | 1 |
| 2/2 | desirable | dot1q | trunking | 1 |

| Port | Vlans allowed on trunk |
|------|------------------------|
| 2/1 | 1-1005 |
| 2/2 | 1-1005 |

| Port | Vlans allowed and active in management domain |
|------|---|
| 2/1 | 1,10,20,30,40,50,60 |
| 2/2 | 1,10,20,30,40,50,60 |

| Port | Vlans in spanning tree forwarding state and not pruned |
|------|--|
| 2/1 | 1,10,20,30,40,50,60 |
| 2/2 | 1,10,20,30,40,50,60 |

Step 4 Use a PING utility program to echo response test the desired ports, VLANs, and ISLs.**Step 5** Go to Chapter 7, “Maintaining the Cisco Catalyst 5500 Multiswitch Router,” and check the MSR equipment status. Replace suspected hardware, then return to Step 1 to verify MSR operation.



Cisco Media Gateway Controller Measurements

Table D-1 provides a list of the ITU measurements available from the Cisco Media Gateway Controller (MGC) through the Cisco TP-Measurement MIB. The information in parenthesis in the MML Counter Name or Components Generating Group column are the associated hexadecimal component type codes found in the component type data file (compType.dat). The logging intervals in this table are all measured in minutes, with the exception of an interval of 24. A logging interval of 24 indicates a 24 hour time period.

Table D-2 provides a list of the ANSI measurements available from the Cisco MGC.

Table D-1 Supported ITU Measurements

| MIB Table Name—
MML Counter Group:Name | Description | MML Counter Name or
Components Generating Gp | Logging
Interval |
|---|---------------------------------------|---|-----------------------------|
| TpTDMIfStatTable—LIF GROUP | Line interface statistics | TDMLnk(x0010)
C7IPLnk (x001d) | |
| LIF: SES, 15/10, 60/30, 24/200 | Number of severely errored seconds | | 15,60,24 |
| LIF: ES | Number of errored seconds | | 15,60,24 |
| LIF: CODE VIOLATION | Number of code violations | | 15,60,24 |
| LIF: FRAME SLIP | Number of frame slips | | 15,60,24 |
| TpTDMLinkStatTable—SC-GROUP | Signaling link statistics | TDMLnk (x0010)
(DPNSS/ISDNPRI only) | |
| SC: XMIT FRM TOT | Total number of frames transmitted | | 15,60,24 |
| SC: RCV FRM TOT | Total number of frames received | | 15,60,24 |
| SC: RCV BAD CRC | Number of bad CRCs received | | 15,60,24 |
| SC: RCV BAD TOT | Total number of bad frames received | | 15,60,24 |
| CHAN BAD TOT 15/10, 60/30, 24/200 | Total number of bad channels | | 15,60,24 |
| SC: RCV FRMR | Number of bad FRMRs received | | 15,60,24 |
| SC: RCV RESET | Number of RESETs received | | 15,60,24 |
| TpTDMAdapterStatTable—DL-GROUP | Data link statistics | Adapter/Card (x0005)
(TDM Only) | |
| DL: RCV UNSOL | Number of unsolicited frames received | | 15,60,24 |
| DL: RCV SABME | Number of SABMEs received | | 15,60,24 |
| CHAN LINK EST 15/10, 60/30, 24/200 | Number of links established | | 15,60,24 |
| DL: XMIT T200 | Number of T200 expires transmitted | | 15,60,24 |
| DL: RCV SEQ | Number of bad N(R) frames received | | 15,60,24 |

Table D-1 Supported ITU Measurements (continued)

| MIB Table Name—
MML Counter Group:Name | Description | MML Counter Name or
Components Generating Gp | Logging
Interval |
|---|---|---|---------------------|
| TpTDMAdapterStatTable—DL-GROUP | Data link statistics (continued) | Adapter/Card (x0005)
(TDM Only) | |
| DL: RCV FRMR RESP | Number of bad frame responses | | 15,60,24 |
| DL: RCV SIZE | Number of bad frame sizes received | | 15,60,24 |
| DL: RCV SABMR | Number of DPNSS SABMR received | | 15,60,24 |
| TpAuxSigServiceStatTable—ASP-GROUP | Auxiliary signal path statistics | AuxSignalingPath (000e) | |
| ASP: XMIT MSG | Number of messages transmitted | | 15,60,24 |
| ASP: RCV MSG | Number of messages received | | 15,60,24 |
| ASP: RCV CONN REQ | Number of call initiate messages received | | 15,60,24 |
| TpSigServiceStatTable—SP-GROUP | Signaling Service statistics | Signaling Services: | |
| SP: cInit in | Number of call init messages received | FAS(x0007) | 15,60,24 |
| SP: cInit out | Number of call init messages sent | SS7/PtCode (x0013) | 15,60,24 |
| SP: PDU in | Number of messages received | NAS (x0014)\ | 15,60,24 |
| SP: PDU out | Number of messages sent | SGCP (x0018) | 15,60,24 |
| SP: Blacklist Call Ctr | Number of blacklist calls counter | EISUP (x0019) | 15,60,24 |
| MDL BLKLST 15/10, 60/30, 24/200 | | AVM (X001b) | 15,60,24 |
| | | VSI (X001c) | 15,60,24 |
| | | IPFAS (x0034) | 15,60,24 |
| | | MGCP(x0035) | |
| TpSS7LinkStatTable—C7LNK-GROUP | SS7 link statistics | LinkSet (x0008) | |
| C7LNK: RCV SU ERR | Number of signaling units received | | 30 |
| C7LNK: XMIT SIO TOT | Number of link realignment (SIF/SIO) messages transmitted | | 30 |
| C7LNK: RCV SIO TOT | Number of link realignment (SIF/SIO) messages received | | 30 |
| C7LNK: DUR IS | Number of seconds C7 link in-service | | 30 |
| C7LNK: DUR UNAVAIL | Number of seconds C7 link unavailable | | 30 |
| C7LNK: MSU DROP-CONG | Number of messages dropped due to congestion | | 30 |
| TpSS7SigServiceStatTable—
C7SP-GROUP | SS7 SignalPath statistics | SS7SigSrvc/PtCode (x0013)
AdjPtCode (x001e) | |
| C7SP: SP DUR UNAVAIL | Number of seconds SP unavailable | | 5,30 |
| C7SP: XMIT MSU DROP/RTE | Number of transmitted messages dropped due to routing failure | | 30 |
| TpPRILinkStatTable—PRI-GROUP | ISDN PRI Link statistics | FASSigSrvc (x0007) | |
| PRI: CHAN MATE UNAVAILABLE | Number of times ISDN PRI link channel mate unavailable | | 15,60,24 |

Table D-1 Supported ITU Measurements (continued)

| MIB Table Name—
MML Counter Group:Name | Description | MML Counter Name or
Components Generating Gp | Logging
Interval |
|---|---------------------------------------|---|---------------------|
| TpISUPSigServiceStatTable—
ISUP-GROUP | ISUP Signaling Service Statistics | Dest PtCode (x0013) | |
| ISUP: XMIT MSG TOT | Number of messages transmitted, total | | 5,30 |
| ISUP: RCV MSG TOT | Number of messages received, total | | 5,30 |
| ISUP: XMIT ACM TOT | Number of ACM messages transmitted | | 5,30 |
| ISUP: RCV ACM TOT | Number of ACM messages received | | 5,30 |
| ISUP: XMIT ANM TOT | Number of ANM messages transmitted | | 5,30 |
| ISUP: RCV ANM TOT | Number of ANM messages received | | 5,30 |
| ISUP: XMIT BLO TOT | Number of BLO messages transmitted | | 5,30 |
| ISUP: RCV BLO TOT | Number of BLO messages received | | 5,30 |
| ISUP: XMIT BLA TOT | Number of BLA messages transmitted | | 5,30 |
| ISUP: RCV BLA TOT | Number of BLA messages received | | 5,30 |
| ISUP: XMIT CPG TOT | Number of CPG messages transmitted | | 5,30 |
| ISUP: RCV CPG TOT | Number of CPG messages received | | 5,30 |
| ISUP: XMIT CGB TOT | Number of CGB messages transmitted | | 5,30 |
| ISUP: RCV CGB TOT | Number of CGB messages received | | 5,30 |
| ISUP: XMIT CGBA TOT | Number of CGBA messages transmitted | | 5,30 |
| ISUP: RCV CGBA TOT | Number of CGBA messages received | | 5,30 |
| ISUP: XMIT GRS TOT | Number of GRS messages transmitted | | 5,30 |
| ISUP: RCV GRS TOT | Number of GRS messages received | | 5,30 |
| ISUP: XMIT GRA TOT | Number of GRA messages transmitted | | 5,30 |
| ISUP: RCV GRA TOT | Number of GRA messages received | | 5,30 |
| ISUP: XMIT CGU TOT | Number of CGU messages transmitted | | 5,30 |
| ISUP: RCV CGU TOT | Number of CGU messages received | | 5,30 |
| ISUP: XMIT CGUA TOT | Number of CGUA messages transmitted | | 5,30 |
| ISUP: RCV CGUA TOT | Number of CGUA messages received | | 5,30 |
| ISUP: XMIT CFN TOT | Number of CFN messages transmitted | | 5,30 |
| ISUP: RCV CFN TOT | Number of CFN messages received | | 5,30 |
| ISUP: XMIT CON TOT | Number of CON messages transmitted | | 5,30 |
| ISUP: RCV CON TOT | Number of CON messages received | | 5,30 |
| ISUP: XMIT IAM TOT | Number of IAM messages transmitted | | 5,30 |
| ISUP: RCV IAM TOT | Number of IAM messages received | | 5,30 |
| ISUP: XMIT INF TOT | Number of INF messages transmitted | | 5,30 |
| ISUP: RCV INF TOT | Number of INF messages received | | 5,30 |

Table D-1 Supported ITU Measurements (continued)

| MIB Table Name—
MML Counter Group:Name | Description | MML Counter Name or
Components Generating Gp | Logging
Interval |
|--|--|---|---------------------|
| TpISUPSigServiceStatTable—
ISUP-GROUP (continued) | ISUP Signaling Service Statistics
(continued) | Dest PtCode (x0013) | |
| ISUP: XMIT INR TOT | Number of INR messages transmitted | | 5,30 |
| ISUP: RCV INR TOT | Number of INR messages received | | 5,30 |
| ISUP: XMIT REL TOT | Number of REL messages transmitted | | 5,30 |
| ISUP: RCV REL TOT | Number of REL messages received | | 5,30 |
| ISUP: XMIT RLC TOT | Number of RLC messages transmitted | | 5,30 |
| ISUP: RCV RLC TOT | Number of RLC messages received | | 5,30 |
| ISUP: XMIT RSC TOT | Number of RSC messages transmitted | | 5,30 |
| ISUP: RCV RSC TOT | Number of RSC messages received | | 5,30 |
| ISUP: XMIT RES TOT | Number of RES messages transmitted | | 5,30 |
| ISUP: RCV RES TOT | Number of RES messages received | | 5,30 |
| ISUP: XMIT SAM TOT | Number of SAM messages transmitted | | 5,30 |
| ISUP: RCV SAM TOT | Number of SAM messages received | | 5,30 |
| ISUP: XMIT SUS TOT | Number of SUS messages transmitted | | 5,30 |
| ISUP: RCV SUS TOT | Number of SUS messages received | | 5,30 |
| ISUP: XMIT UBL TOT | Number of UBL messages transmitted | | 5,30 |
| ISUP: RCV UBL TOT | Number of UBL messages received | | 5,30 |
| ISUP: XMIT UBA TOT | Number of UBA messages transmitted | | 5,30 |
| ISUP: RCV UBA TOT | Number of UBA messages received | | 5,30 |
| ISUP: XMIT USR TOT | Number of USR messages transmitted | | 5,30 |
| ISUP: RCV USR TOT | Number of USR messages received | | 5,30 |
| ISUP: XMIT CCR TOT | Number of CCR messages transmitted | | 5,30 |
| ISUP: RCV CCR TOT | Number of CCR messages received | | 5,30 |
| ISUP: XMIT COT TOT | Number of COT messages transmitted | | 5,30 |
| ISUP: RCV COT TOT | Number of COT messages received | | 5,30 |
| ISUP: XMIT CQM TOT | Number of CQM messages transmitted | | 5,30 |
| ISUP: RCV CQM TOT | Number of CQM messages received | | 5,30 |
| ISUP: XMIT CQR TOT | Number of CQR messages transmitted | | 5,30 |
| ISUP: RCV CQR TOT | Number of CQR messages received | | 5,30 |
| ISUP: XMIT CRA TOT | Number of CRA messages transmitted | | 5,30 |
| ISUP: RCV CRA TOT | Number of CRA messages received | | 5,30 |
| ISUP: XMIT CRM TOT | Number of CRM messages transmitted | | 5,30 |
| ISUP: RCV CRM TOT | Number of CRM messages received | | 5,30 |

Table D-1 Supported ITU Measurements (continued)

| MIB Table Name—
MML Counter Group:Name | Description | MML Counter Name or
Components Generating Gp | Logging
Interval |
|--|--|---|---------------------|
| TpISUPSigServiceStatTable—
ISUP-GROUP (continued) | ISUP Signaling Service Statistics
(continued) | Dest PtCode (x0013) | |
| ISUP: XMIT CVR TOT | Number of CVR messages transmitted | | 5,30 |
| ISUP: RCV CVR TOT | Number of CVR messages received | | 5,30 |
| ISUP: XMIT CVT TOT | Number of CVT messages transmitted | | 5,30 |
| ISUP: RCV CVT TOT | Number of CVT messages received | | 5,30 |
| ISUP: XMIT EXM TOT | Number of EXM messages transmitted | | 5,30 |
| ISUP: RCV EXM TOT | Number of EXM messages received | | 5,30 |
| ISUP: XMIT FAC TOT | Number of FAC messages transmitted | | 5,30 |
| ISUP: RCV FAC TOT | Number of FAC messages received | | 5,30 |
| ISUP: XMIT FOT TOT | Number of FOT messages transmitted | | 5,30 |
| ISUP: RCV FOT TOT | Number of FOT messages received | | 5,30 |
| ISUP: XMIT LPA TOT | Number of LPA messages transmitted | | 5,30 |
| ISUP: RCV LPA TOT | Number of LPA messages received | | 5,30 |
| ISUP: XMIT PAM TOT | Number of PAM messages transmitted | | 5,30 |
| ISUP: RCV PAM TOT | Number of PAM messages received | | 5,30 |
| ISUP: XMIT UCIC TOT | Number of UCIC messages transmitted | | 5,30 |
| ISUP: RCV UCIC TOT | Number of UCIC messages received | | 5,30 |
| ISUP: XMIT FAA TOT | Number of FAA messages transmitted | | 5,30 |
| ISUP: RCV FAA TOT | Number of FAA messages received | | 5,30 |
| ISUP: XMIT FAD TOT | Number of FAD messages transmitted | | 5,30 |
| ISUP: RCV FAD TOT | Number of FAD messages received | | 5,30 |
| ISUP: XMIT FAR TOT | Number of FAR messages transmitted | | 5,30 |
| ISUP: RCV FAR TOT | Number of FAR messages received | | 5,30 |
| ISUP: XMIT FRJ TOT | Number of FRJ messages transmitted | | 5,30 |
| ISUP: RCV FRJ TOT | Number of FRJ messages received | | 5,30 |
| ISUP: XMIT SGM TOT | Number of SGM messages transmitted | | 5,30 |
| ISUP: RCV SGM TOT | Number of SGM messages received | | 5,30 |
| ISUP: XMIT MPM TOT | Number of MPM messages transmitted | | 5,30 |
| ISUP: RCV MPM TOT | Number of MPM messages received | | 5,30 |
| ISUP: ABN REL TOT | Number of abnormal clear messages
received | | 5,30 |
| ISUP: UNEX MSG TOT | Number of unexpected messages
received | | 5,30 |

Table D-1 Supported ITU Measurements (continued)

| MIB Table Name—
MML Counter Group:Name | Description | MML Counter Name or
Components Generating Gp | Logging
Interval |
|--|---|---|---------------------|
| TpISUPSigServiceStatTable—
ISUP-GROUP (continued) | ISUP Signaling Service Statistics
(continued) | Dest PtCode (x0013) | |
| ISUP: UNREC MSG TOT | Number of unrecognized messages
received | | 5,30 |
| ISUP: CHAN MATE
UNAVAILABLE | Number of Channel Mate Unavailable
messages received | | 5,30 |
| TpTUPSigServiceStatTable—
TUP-GROUP | Telephone User Part statistics | Dest PtCode (x0013) | |
| TUP: XMIT MSG TOT | Number of messages transmitted, total | | 5,30 |
| TUP: RCV MSG TOT | Number of messages received, total | | 5,30 |
| TUP: XMIT ACB TOT | Number of ACB messages transmitted | | 5,30 |
| TUP: RCV ACB TOT | Number of ACB messages received | | 5,30 |
| TUP: XMIT ACC TOT | Number of ACC messages transmitted | | 5,30 |
| TUP: RCV ACC TOT | Number of ACC messages received | | 5,30 |
| TUP: XMIT ACM TOT | Number of ACM messages transmitted | | 5,30 |
| TUP: RCV ACM TOT | Number of ACM messages received | | 5,30 |
| TUP: XMIT CBK TOT | Number of CBK messages transmitted | | 5,30 |
| TUP: RCV CBK TOT | Number of CBK messages received | | 5,30 |
| TUP: XMIT CCF TOT | Number of CCF messages transmitted | | 5,30 |
| TUP: RCV CCF TOT | Number of CCF messages received | | 5,30 |
| TUP: XMIT CCL TOT | Number of CCL messages transmitted | | 5,30 |
| TUP: RCV CCL TOT | Number of CCL messages received | | 5,30 |
| TUP: XMIT CCR TOT | Number of CCR messages transmitted | | 5,30 |
| TUP: RCV CCR TOT | Number of CCR messages received | | 5,30 |
| TUP: XMIT CFL TOT | Number of CFL messages transmitted | | 5,30 |
| TUP: RCV CFL TOT | Number of CFL messages received | | 5,30 |
| TUP: XMIT CGC TOT | Number of CGC messages transmitted | | 5,30 |
| TUP: RCV CGC TOT | Number of CGC messages received | | 5,30 |
| TUP: XMIT CHG TOT | Number of CHG messages transmitted | | 5,30 |
| TUP: RCV CHG TOT | Number of CHG messages received | | 5,30 |
| TUP: XMIT COT TOT | Number of COT messages transmitted | | 5,30 |
| TUP: RCV COT TOT | Number of COT messages received | | 5,30 |
| TUP: XMIT DPN TOT | Number of DPN messages transmitted | | 5,30 |
| TUP: RCV DPN TOT | Number of DPN messages received | | 5,30 |
| TUP: XMIT EUM TOT | Number of EUM messages transmitted | | 5,30 |
| TUP: RCV EUM TOT | Number of EUM messages received | | 5,30 |

Table D-1 Supported ITU Measurements (continued)

| MIB Table Name—
MML Counter Group:Name | Description | MML Counter Name or
Components Generating Gp | Logging
Interval |
|--|---|---|---------------------|
| TpTUPSigServiceStatTable—
TUP-GROUP (continued) | Telephone User Part statistics
(continued) | Dest PtCode (x0013) | |
| TUP: XMIT FOT TOT | Number of FOT messages transmitted | | 5,30 |
| TUP: RCV FOT TOT | Number of FOT messages received | | 5,30 |
| TUP: XMIT GRA TOT | Number of GRA messages transmitted | | 5,30 |
| TUP: RCV GRA TOT | Number of GRA messages received | | 5,30 |
| TUP: XMIT GRQ TOT | Number of GRQ messages transmitted | | 5,30 |
| TUP: RCV GRQ TOT | Number of GRQ messages received | | 5,30 |
| TUP: XMIT GRS TOT | Number of GRS messages transmitted | | 5,30 |
| TUP: RCV GRS TOT | Number of GRS messages received | | 5,30 |
| TUP: XMIT GSM TOT | Number of GSM messages transmitted | | 5,30 |
| TUP: RCV GSM TOT | Number of GSM messages received | | 5,30 |
| TUP: XMIT HBA TOT | Number of HBA messages transmitted | | 5,30 |
| TUP: RCV HBA TOT | Number of HBA messages received | | 5,30 |
| TUP: XMIT HGB TOT | Number of HGB messages transmitted | | 5,30 |
| TUP: RCV HGB TOT | Number of HGB messages received | | 5,30 |
| TUP: XMIT HGU TOT | Number of HGU messages transmitted | | 5,30 |
| TUP: RCV HGU TOT | Number of HGU messages received | | 5,30 |
| TUP: XMIT HUA TOT | Number of HUA messages transmitted | | 5,30 |
| TUP: RCV HUA TOT | Number of HUA messages received | | 5,30 |
| TUP: XMIT IAI TOT | Number of IAI messages transmitted | | 5,30 |
| TUP: RCV IAI TOT | Number of IAI messages received | | 5,30 |
| TUP: XMIT IAM TOT | Number of IAM messages transmitted | | 5,30 |
| TUP: RCV IAM TOT | Number of IAM messages received | | 5,30 |
| TUP: XMIT LOS TOT | Number of LOS messages transmitted | | 5,30 |
| TUP: RCV LOS TOT | Number of LOS messages received | | 5,30 |
| TUP: XMIT MAL TOT | Number of MAL messages transmitted | | 5,30 |
| TUP: RCV MAL TOT | Number of MAL messages received | | 5,30 |
| TUP: XMIT MBA TOT | Number of MBA messages transmitted | | 5,30 |
| TUP: RCV MBA TOT | Number of MBA messages received | | 5,30 |
| TUP: XMIT MGB TOT | Number of MGB messages transmitted | | 5,30 |
| TUP: RCV MGB TOT | Number of MGB messages received | | 5,30 |
| TUP: XMIT MGU TOT | Number of MGU messages transmitted | | 5,30 |
| TUP: RCV MGU TOT | Number of MGU messages received | | 5,30 |

Table D-1 Supported ITU Measurements (continued)

| MIB Table Name—
MML Counter Group:Name | Description | MML Counter Name or
Components Generating Gp | Logging
Interval |
|--|---|---|---------------------|
| TpTUPSigServiceStatTable—
TUP-GROUP (continued) | Telephone User Part statistics
(continued) | Dest PtCode (x0013) | |
| TUP: XMIT MPM TOT | Number of MPM messages transmitted | | 5,30 |
| TUP: RCV MPM TOT | Number of MPM messages received | | 5,30 |
| TUP: XMIT MUA TOT | Number of MUA messages transmitted | | 5,30 |
| TUP: RCV MUA TOT | Number of MUA messages received | | 5,30 |
| TUP: XMIT NNC TOT | Number of NCC messages transmitted | | 5,30 |
| TUP: RCV NNC TOT | Number of NCC messages received | | 5,30 |
| TUP: XMIT OPR TOT | Number of OPR messages transmitted | | 5,30 |
| TUP: RCV OPR TOT | Number of OPR messages received | | 5,30 |
| TUP: XMIT RAN TOT | Number of RAN messages transmitted | | 5,30 |
| TUP: RCV RAN TOT | Number of RAN messages received | | 5,30 |
| TUP: XMIT RLG TOT | Number of RLG messages transmitted | | 5,30 |
| TUP: RCV RLG TOT | Number of RLG messages received | | 5,30 |
| TUP: XMIT RSC TOT | Number of RSC messages transmitted | | 5,30 |
| TUP: RCV RSC TOT | Number of RSC messages received | | 5,30 |
| TUP: XMIT SAM TOT | Number of SAM messages transmitted | | 5,30 |
| TUP: RCV SAM TOT | Number of SAM messages received | | 5,30 |
| TUP: XMIT SAO TOT | Number of SAO messages transmitted | | 5,30 |
| TUP: RCV SAO TOT | Number of SAO messages received | | 5,30 |
| TUP: XMIT SBA TOT | Number of SBA messages transmitted | | 5,30 |
| TUP: RCV SBA TOT | Number of SBA messages received | | 5,30 |
| TUP: XMIT SEC TOT | Number of SEC messages transmitted | | 5,30 |
| TUP: RCV SEC TOT | Number of SEC messages received | | 5,30 |
| TUP: XMIT SGB TOT | Number of SGB messages transmitted | | 5,30 |
| TUP: RCV SGB TOT | Number of SGB messages received | | 5,30 |
| TUP: XMIT SGU TOT | Number of SGU messages transmitted | | 5,30 |
| TUP: RCV SGU TOT | Number of SGU messages received | | 5,30 |
| TUP: XMIT SLB TOT | Number of SLB messages transmitted | | 5,30 |
| TUP: RCV SLB TOT | Number of SLB messages received | | 5,30 |
| TUP: XMIT SSB TOT | Number of SSB messages transmitted | | 5,30 |
| TUP: RCV SSB TOT | Number of SSB messages received | | 5,30 |
| TUP: XMIT SST TOT | Number of SST messages transmitted | | 5,30 |
| TUP: RCV SST TOT | Number of SST messages received | | 5,30 |

Table D-1 Supported ITU Measurements (continued)

| MIB Table Name—
MML Counter Group:Name | Description | MML Counter Name or
Components Generating Gp | Logging
Interval |
|--|---|---|---------------------|
| TpTUPSigServiceStatTable—
TUP-GROUP (continued) | Telephone User Part statistics
(continued) | Dest PtCode (x0013) | |
| TUP: XMIT STB TOT | Number of STB messages transmitted | | 5,30 |
| TUP: RCV STB TOT | Number of STB messages received | | 5,30 |
| TUP: XMIT SUA TOT | Number of SUA messages transmitted | | 5,30 |
| TUP: RCV SUA TOT | Number of SUA messages received | | 5,30 |
| TUP: XMIT UBA TOT | Number of UBA messages transmitted | | 5,30 |
| TUP: RCV UBA TOT | Number of UBA messages received | | 5,30 |
| TUP: XMIT UBL TOT | Number of UBL messages transmitted | | 5,30 |
| TUP: RCV UBL TOT | Number of UBL messages received | | 5,30 |
| TUP: XMIT UNN TOT | Number of UNN messages transmitted | | 5,30 |
| TUP: RCV UNN TOT | Number of UNN messages received | | 5,30 |
| TUP: ABN REL TOT | Number of abnormal clear messages
received | | 5,30 |
| TUP: UNEXP MSG TOT | Number of unexpected messages
received | | 5,30 |
| TUP: UNREC MSG TOT | Number of unrecognized messages
received | | 5,30 |
| TUP: CHAN MATE UNAVAILABLE | Number of Channel Mate Unavailable
messages received | | 5,30 |
| TpNUPSigServiceStatTable—
NUP-GROUP | National User Part Statistics | Dest PtCode (x0013) | |
| NUP: XMIT MSG TOT | Number of messages transmitted, total | | 5,30 |
| NUP: RCV MSG TOT | Number of messages received, total | | 5,30 |
| NUP: UNEX MSG TOT | Number of unexpected messages
received | | 5,30 |
| TpOVLStatTable—OVL-GROUP | OverLoad Statistics | MGC NE (x0001) | |
| OVL: LVL1 Duration | Number of minutes in level 1 overload
condition | | 15,60,24 |
| OVL: LVL2 Duration | Number of minutes in level 2 overload
condition | | 15,60,24 |
| OVL: LVL3 Duration | Number of minutes in level 3 overload
condition | | 15,60,24 |
| OVL: Call Failure | Number of calls rejected due to
overload condition (measurement is
removed as of release 7.4(11)) | | 15,60,24 |

Table D-1 Supported ITU Measurements (continued)

| MIB Table Name—
MML Counter Group:Name | Description | MML Counter Name or
Components Generating Gp | Logging
Interval |
|---|----------------------------|---|---------------------|
| TpSystemStatTable—STATE-GROUP | User Defined Statistics | MGC NE (x0001) | |
| STATE: CDB ReCord Xmit | Number of CDBs transmitted | | 15,60,24 |
| STATE: User Count1 | User defined count 1 | | 15,60,24 |
| STATE: User Count2 | User defined count 2 | | 15,60,24 |
| STATE: User Count3 | User defined count 3 | | 15,60,24 |
| STATE: User Count4 | User defined count 4 | | 15,60,24 |
| STATE: User Count5 | User defined count 5 | | 15,60,24 |
| STATE: User Count6 | User defined count 6 | | 15,60,24 |
| STATE: User Count7 | User defined count 7 | | 15,60,24 |
| STATE: User Count8 | User defined count 8 | | 15,60,24 |
| STATE:User Count 9 | User defined count 9 | | 15,60,24 |
| STATE: User Count10 | User defined count 10 | | 15,60,24 |
| STATE: User Count11 | User defined count 11 | | 15,60,24 |
| STATE: User Count12 | User defined count 12 | | 15,60,24 |
| STATE: User Count13 | User defined count 13 | | 15,60,24 |
| STATE: User Count14 | User defined count 14 | | 15,60,24 |
| STATE: User Count15 | User defined count 15 | | 15,60,24 |
| STATE: User Count16 | User defined count 16 | | 15,60,24 |
| STATE: User Count17 | User defined count 17 | | 15,60,24 |
| STATE: User Count18 | User defined count 18 | | 15,60,24 |
| STATE: User Count19 | User defined count 19 | | 15,60,24 |
| STATE: User Count20 | User defined count 20 | | 15,60,24 |
| STATE: User Count21 | User defined count 21 | | 15,60,24 |
| STATE: User Count22 | User defined count 22 | | 15,60,24 |
| STATE: User Count23 | User defined count 23 | | 15,60,24 |
| STATE: User Count24 | User defined count 24 | | 15,60,24 |
| STATE: User Count25 | User defined count 25 | | 15,60,24 |

Table D-1 Supported ITU Measurements (continued)

| MIB Table Name—
MML Counter Group:Name | Description | MML Counter Name or
Components Generating Gp | Logging
Interval |
|---|--|---|---------------------|
| tpTCAPStatTable—TCAP-GROUP | Transaction Capabilities Application
Part statistics | MGC NE (x0001) | |
| TCAP: MSG XMIT | Total number of messages transmitted | | 5,30 |
| TCAP: QWP XMIT | Number of Query with permission
messages transmitted | | 5,30 |
| TCAP: RSP XMIT | Number of Response messages
transmitted | | 5,30 |
| TCAP: UNI XMIT | Number of Unidirectional messages
transmitted | | 5,30 |
| TCAP: ABT XMIT | Number of Abort messages transmitted | | 5,30 |
| TCAP: MSG RCV | Total number of messages received | | 5,30 |
| TCAP: QWP RCV | Number of Query with permission
messages received | | 5,30 |
| TCAP: RSP RCV | Number of Response messages
received | | 5,30 |
| TCAP: UNI RCV | Number of Unidirectional messages
received | | 5,30 |
| TCAP: ABT RCV | Number of Abort messages received | | 5,30 |
| TCAP: MSG DROP | Number of messages dropped | | 5,30 |
| TCAP: MSG UNREC | Number of unrecognized messages
received | | 5,30 |
| TCAP: BEGIN XMIT | Number of Begin messages
transmitted. This measurement is valid
only for ETSI and ITU TCAP. | | 5,30 |
| TCAP: BEGIN RCV | Number of Begin messages received.
This measurement is valid only for
ETSI and ITU TCAP. | | 5,30 |
| TCAP: END XMIT | Number of End messages transmitted.
This measurement is valid only for
ETSI and ITU TCAP. | | 5,30 |
| TCAP: END RCV | Number of End messages received.
This measurement is valid only for
ETSI and ITU TCAP. | | 5,30 |
| TCAP: CONTINUE XMIT | Number of Continue messages
transmitted. This measurement is valid
only for ETSI and ITU TCAP. | | 5,30 |
| TCAP: CONTINUE RCV | Number of Continue messages
received. This measurement is valid
only for ETSI and ITU TCAP. | | 5,30 |

Table D-1 Supported ITU Measurements (continued)

| MIB Table Name—
MML Counter Group:Name | Description | MML Counter Name or
Components Generating Gp | Logging
Interval |
|---|--|---|---------------------|
| tpTCAPStatTable—TCAP-GROUP
(continued) | Transaction Capabilities Application
Part statistics (continued) | MGC NE (x0001) | |
| TCAP: CONV XMIT | Number of Conversation messages
transmitted. This measurement is valid
only for ANSI TCAP. | | 5,30 |
| TCAP: CONV RCV | Number of Conversation messages
received. This measurement is valid
only for ANSI TCAP. | | 5,30 |
| tpCALLStatTable—CALL-GROUP
(new as of release 7.4(11)) | Call Statistics | MGC NE (x0001) | |
| CALL: SuccCall TOT | Number successful calls | | 15,60,24 |
| CALL: FailCall TOT | Number failed calls | | 15,60,24 |
| CALL: RUFailCall TOT | Number of failed calls due to a
resource being unavailable | | 15,60,24 |
| CALL: ORFailCall TOT | Number of failed calls due to other
reasons | | 15,60,24 |
| CALL: OLFailCall TOT | Number of calls rejected due to
overload condition | | 15,60,24 |
| tpSCCPStatTable—SCCP-GROUP | Signaling Connection Control Part
statistics | MGC NE (x0001) | |
| SCCP:ROUTING FAILURE | Total number of routing failures | | 5,30 |
| SCCP: UDT XMIT | Number of unit data messages
transmitted | | 5,30 |
| SCCP: UDTS XMIT | Number of unit data service messages
transmitted | | 5,30 |
| SCCP: UDT RCV | Number of unit data messages received | | 5,30 |
| SCCP: UDTS RCV | Number of unit data service messages
received | | 5,30 |
| SCCP: TOTAL MSG | Total number of messages handled | | 5,30 |

ANSI ISUP Measurements

Table D-2 provides a list of the ANSI ISDN User Part (ISUP) measurements available from the Cisco Media Gateway Controller.

Table D-2 Supported ANSI ISUP Measurements

| ANSI Measurement Name | MML Counter Group:Name | Description |
|------------------------------|-------------------------------|---|
| CountSentMessages | ISUP: XMIT MSG TOT | count of every message sent |
| CountReceivedMessages | ISUP: RCV MSG TOT | count of every message received |
| CountSentACM | ISUP: XMIT ACM TOT | count of every Address Complete Message (ACM) received |
| CountReceivedACM | ISUP: RCV ACM TOT | count of every ACM sent |
| CountSentANM | ISUP: XMIT ANM TOT | count of every Answer Message (ANM) received |
| CountReceivedANM | ISUP: RCV ANM TOT | count of every ANM sent |
| CountSentBLO | ISUP: XMIT BLO TOT | count of every Blocking (BLO) message received |
| CountReceivedBLO | ISUP: RCV BLO TOT | count of every BLO message sent |
| CountSentBLA | ISUP: XMIT BLA TOT | count of every Blocking Acknowledgement (BLA) message received |
| CountReceivedBLA | ISUP: RCV BLA TOT | count of every BLA message sent |
| CountSentCCR | ISUP: XMIT CCR TOT | count of every Current Cell Rate (CCR) message received |
| CountReceivedCCR | ISUP: RCV CCR TOT | count of every CCR message sent |
| CountSentCFN | ISUP: XMIT CFN TOT | count of every Confusion (CFN) message received |
| CountReceivedCFN | ISUP: RCV CFN TOT | count of every CFN message sent |
| CountSentCGB | ISUP: XMIT CGB TOT | count of every Circuit Group Blocking (CGB) message received |
| CountReceivedCGB | ISUP: RCV CGB TOT | count of every CGB message sent |
| CountSentCGBA | ISUP: XMIT CGBA TOT | count of every Circuit Group Blocking Acknowledgement (CGBA) message received |
| CountReceivedCGBA | ISUP: RCV CGBA TOT | count of every CGBA message sent |
| CountSentCGU | ISUP: XMIT CGU TOT | count of every Circuit Group Unblocking (CGU) message received |
| CountReceivedCGU | ISUP: RCV CGU TOT | count of every CGU message sent |

Table D-2 Supported ANSI ISUP Measurements (continued)

| ANSI Measurement Name | MML Counter Group:Name | Description |
|------------------------------|-------------------------------|---|
| CountSentCGUA | ISUP: XMIT CGUA TOT | count of every Circuit Group Unblocking Acknowledgement (CGUA) message received |
| CountReceivedCGUA | ISUP: RCV CGUA TOT | count of every CGUA sent |
| CountSentCOT | ISUP: XMIT COT TOT | count of every Continuity Check (COT) message received |
| CountReceivedCOT | ISUP: RCV COT TOT | count of every COT message sent |
| CountSentCPG | ISUP: XMIT CPG TOT | count of every Call Progress (CPG) message received |
| CountReceivedCPG | ISUP: RCV CPG TOT | count of every CPG message sent |
| CountSentCQM | ISUP: XMIT CQM TOT | count of every Circuit Group Query Message (CQM) received |
| CountReceivedCQM | ISUP: RCV CQM TOT | count of every CQM sent |
| CountSentCQR | ISUP: XMIT CQR TOT | count of every Circuit Group Query Response (CQR) message received |
| CountReceivedCQR | ISUP: RCV CQR TOT | count of every CQR message sent |
| CountSentCRA | ISUP: XMIT CRA TOT | count of every Circuit Reservation Acknowledgement (CRA) message received |
| CountReceivedCRA | ISUP: RCV CRA TOT | count of every CRA message sent |
| CountSentCRM | ISUP: XMIT CRM TOT | count of every Cell Rate Margin (CRM) message received |
| CountReceivedCRM | ISUP: RCV CRM TOT | count of every CRM message sent |
| CountSentCVR | ISUP: XMIT CVR TOT | count of every Circuit Validation Response (CVR) message received |
| CountReceivedCVR | ISUP: RCV CVR TOT | count of every CVR message sent |
| CountSentCVT | ISUP: XMIT CVT TOT | count of every Circuit Validation Test (CVT) message received |
| CountReceivedCVT | ISUP: RCV CVT TOT | count of every CVT message sent |
| CountSentEXM | ISUP: XMIT EXM TOT | count of every Exit Message (EXM) received |
| CountReceivedEXM | ISUP: RCV EXM TOT | count of every EXM sent |
| CountSentFAC | ISUP: XMIT FAC TOT | count of every Facility (FAC) message received |
| CountReceivedFAC | ISUP: RCV FAC TOT | count of every FAC message sent |

Table D-2 Supported ANSI ISUP Measurements (continued)

| ANSI Measurement Name | MML Counter Group:Name | Description |
|------------------------------|-------------------------------|--|
| CountSentFOT | ISUP: XMIT FOT TOT | count of every Forward Transfer (FOT) message received |
| CountReceivedFOT | ISUP: RCV FOT TOT | count of every FOT message sent |
| CountSentGRS | ISUP: XMIT GRS TOT | count of every Circuit Group Reset (GRS) message received |
| CountReceivedGRS | ISUP: RCV GRS TOT | count of every GRS message sent |
| CountSentGRA | ISUP: XMIT GRA TOT | count of every Circuit Group Reset Acknowledgment (GRA) message received |
| CountReceivedGRA | ISUP: RCV GRA TOT | count of every GRA message sent |
| CountSentIAM | ISUP: XMIT IAM TOT | count of every Initial Address Message (IAM) received |
| CountReceivedIAM | ISUP: RCV IAM TOT | count of every IAM sent |
| CountSentINF | ISUP: XMIT INF TOT | count of every INF received |
| CountReceivedINF | ISUP: RCV INF TOT | count of every INF sent |
| CountSentINR | ISUP: XMIT INR TOT | count of every INR received |
| CountReceivedINR | ISUP: RCV INR TOT | count of every INR sent |
| CountSentLPA | ISUP: XMIT LPA TOT | count of every Loop Back Acknowledgement (LPA) message received |
| CountReceivedLPA | ISUP: RCV LPA TOT | count of every LPA message sent |
| CountSentPAM | ISUP: XMIT PAM TOT | count of every Pass Along Message (PAM) received |
| CountReceivedPAM | ISUP: RCV PAM TOT | count of every PAM sent |
| CountSentREL | ISUP: XMIT REL TOT | count of every Release (REL) message received |
| CountReceivedREL | ISUP: RCV REL TOT | count of every REL message sent |
| CountSentRLC | ISUP: XMIT RLC TOT | count of every Release Complete (RLC) received |
| CountReceivedRLC | ISUP: RCV RLC TOT | count of every RLC message sent |
| CountSentRSC | ISUP: XMIT RSC TOT | count of every Reset Circuit (RSC) message received |
| CountReceivedRSC | ISUP: RCV RSC TOT | count of every RSC message sent |
| CountSentRES | ISUP: XMIT RES TOT | count of every Resume (RES) message received |
| CountReceivedRES | ISUP: RCV RES TOT | count of every RES message sent |
| CountSentSUS | ISUP: XMIT SUS TOT | count of every Suspend (SUS) message received |
| CountReceivedSUS | ISUP: RCV SUS TOT | count of every SUS message sent |

Table D-2 Supported ANSI ISUP Measurements (continued)

| ANSI Measurement Name | MML Counter Group:Name | Description |
|------------------------------|-------------------------------|---|
| CountSentUBL | ISUP: XMIT UBL TOT | count of every Unblocking (UBL) message received |
| CountReceivedUBL | ISUP: RCV UBL TOT | count of every UBL message sent |
| CountSentUBA | ISUP: XMIT UBA TOT | count of every Unblocking Acknowledgement (UBA) message received |
| CountReceivedUBA | ISUP: RCV UBA TOT | count of every UBA message received |
| CountSentUCIC | ISUP: XMIT UCIC TOT | count of every Unequipped Carrier Identification Code (UCIC) message sent |
| CountReceivedUCIC | ISUP: RCV UCIC TOT | count of every UCIC message received |
| CountSentUSR | ISUP: XMIT USR TOT | count of every User-to-User Information (USR) message sent |
| CountReceivedUSR | ISUP: RCV USR TOT | count of every USR message received |
| CountAbnormalReleases | ISUP: ABN REL TOT | count of release messages not normal clearing |
| CountUnexpectedMsg | ISUP: UNEX MSG TOT | count of unexpected messages |
| CountUnrecognizedMsg | ISUP: UNREC MSG TOT | count of unrecognized messages |
| CountMatedChanUnavailable | ISUP: CHAN MATE UNAVAILABLE | count of when B mate not there |



A

ACC

- alarm associations for ACC overload levels (table) **3-77**
- CPU timer interval parameter **3-78**
- managing **3-75**
- maximum ACL mapping values (table) **3-79**
- maximum ACL value **3-78**
- maximum ACL value, modifying **3-79**
- overload level, retrieving **3-80**
- overload level percentage parameters **3-75**

AC power supply

- front panels (figure) **7-9**
- handling (figure) **7-10**
- installing **7-10**
- removal and replacement **7-8**
- removing **7-9**

administrative state

- CICs, retrieving **3-62**
- CICs, setting **8-75**
- Cisco MGC, retrieving **3-59**
- Cisco MGC, setting **8-71**
- media gateway, retrieving **3-60**
- media gateway, setting **8-71**
- retrieving **3-59**
- signaling service, retrieving **3-60**
- signaling service, setting **8-73**
- spans, retrieving **3-61**
- spans, setting **8-73**
- trunk group, retrieving **3-60**
- trunk group, setting **8-72**

alarm and measurement viewer

- alarm record view tab window (figure) **3-106**

- meas record view tab window (figure) **3-104**

- using **3-103**

- viewing and searching alarm **3-105**

- viewing and searching measurements **3-104**

- alarm record view tab window (figure) **3-106**

alarms

- acknowledging **8-3**
- All C7 IP Links Fail resolution **8-9**
- All Conn Cntl Links Fail resolution **8-8**
- All ISDN IP Conn Fail resolution **8-10**
- ANAL: ALoopCtrExceeded **8-11**
- ANAL: ATableFail_GetDigMod resolution **8-12**
- ANAL: ATableFail_GetDigTree resolution **8-11**
- ANAL: ATableFail_GetResult resolution **8-12**
- ANAL: BLoopCtrExceeded resolution **8-12**
- ANAL: BNum_GetFail_SrvCtbl resolution **8-12**
- ANAL: BNum_MdfyBFail_AnnounceID resolution **8-13**
- ANAL: BTableFail_GetDigMod resolution **8-13**
- ANAL: BTableFail_GetDigTree resolution **8-13**
- ANAL: BTableFail_GetResult resolution **8-14**
- ANAL: Cause_GetFail_CauseTbl resolution **8-14**
- ANAL: Cause_GetFail_DigModTbl resolution **8-14**
- ANAL: Cause_GetFail_InvldRsltType resolution **8-15**
- ANAL: Cause_GetFail_LocTbl resolution **8-15**
- ANAL: Cause_GetFail_RsltTbl resolution **8-15**
- ANAL: Cause_InvldRsIts_CauseTbl resolution **8-16**
- ANAL: Cause_MdfyBFail_AnnounceID resolution **8-16**
- ANAL: Cause_MdfyBFail_AppPtInvld resolution **8-16**
- ANAL: Cause_Rte_LoopDetected resolution **8-17**
- ANAL: CustId/StartIdx Missing resolution **8-17**
- ANAL: Data Failure Rcvd resolution **8-19**
- ANAL: InvalidtrkGrpType resolution **8-19**

- ANAL: Prof_GetFail_DigModTbl resolution **8-20**
- ANAL: Prof_GetFail_InvldRslt resolution **8-20**
- ANAL: Prof_GetFail_NOATbl resolution **8-20**
- ANAL: Prof_GetFail_NPITbl resolution **8-21**
- ANAL: Prof_GetFail_RsltTbl resolution **8-21**
- ANAL: Prof_InvldNPATbl resolution **8-22**
- ANAL: Prof_InvRslts_NOATbl resolution **8-22**
- ANAL: Prof_MdfyBFail_AppPtInvld resolution **8-22**
- ANAL: RteStartIndexInvalid resolution **8-23**
- ANAL: RteTableFail_GetRteList resolution **8-23**
- ANAL: RteTableFail_GetTrkAttrdata resolution **8-23**
- ANAL: RteTableFail_GetTrkGrpdata resolution **8-24**
- ANAL: RteTableFail_GetTrunkList resolution **8-24**
- ANAL: TrunkGrpRsltCtrExceeded resolution **8-24**
- archived, field descriptions (table) **A-6**
- associations for ACC overload levels (table) **3-77**
- C7DPC CONGESTION resolution **8-24**
- C7LNK ALGNMT LOST resolution **8-24**
- C7LNK CONGESTION resolution **8-25**
- C7LNK INHIBIT resolution **8-25**
- category data, retrieving **3-87**
- clearing **8-4**
- Config Fail resolution **8-26**
- data dumper, configuring **A-2**
- DISK resolution **8-26**
- dumper sink log file parameters (table) **A-3**
- Ext Node Interface Fail resolution **8-26**
- FailoverPeerLost resolution **8-27**
- FailoverPeerOOS resolution **8-28**
- FAIL resolution **8-27**
- Gen Fail resolution **8-28**
- IP CONNECTION FAILED resolution **8-29**
- IP RTE CONF FAIL resolution **8-30**
- IP RTE FAIL resolution **8-30**
- ISUP: COT Failure resolution **8-31**
- LIF: IDLE CHANGE resolution **8-34**
- LIF: LOST CD resolution **8-34**
- LIF: LOST CTS resolution **8-34**
- LIF BER resolution **8-31**
- LIF FAIL resolution **8-31**
- LIF LOF resolution **8-32**
- LIF LOS resolution **8-32**
- LIF SES resolution **8-33**
- LIF YELLOW resolution **8-33**
- MMDB: Database cause failover resolution **8-35**
- MMDB: Database nearly full resolution **8-35**
- MMDB: Database unavailable resolution **8-35**
- NAS: AuditResponse Failure resolution **8-35**
- NAS: CommsFailure resolution **8-36**
- NAS: ResourceFailure resolution **8-37**
- OOS TRAFFIC RE-ROUTE resolution **8-37**
- OverloadHeavy resolution **8-38**
- OverloadLight resolution **8-39**
- OverloadMedium resolution **8-38**
- PC UNAVAIL resolution **8-39**
- Peer IP Links Failure resolution **8-39**
- PEER LINK A FAILURE resolution **8-40**
- PEER LINK B FAILURE resolution **8-40**
- PEER MODULE FAILURE resolution **8-40**
- POM: DynamicReconfiguration resolution **8-41**
- POM: PEER_SYNC_ERR resolution **8-41**
- POM INACTIVITY TIMEOUT resolution **8-41**
- POM SESSION TERMINATE resolution **8-41**
- PRI:B-Channel not available resolution **8-41**
- ProcM No Response resolution **8-42**
- REPL: all connections failure resolution **8-42**
- retrieving all **8-3**
- RSET CONFIG FAIL resolution **8-43**
- SC CONFIG FAIL resolution **8-43**
- SC FAIL resolution **8-44**
- SC M-OOS resolution **8-44**
- SRCP audit, resolution **8-97**
- srcpAudit: GwBackhaulProto resolution **8-44**
- srcpAudit: GwBackhaulSes resolution **8-45**
- srcpAudit: GwControlProto resolution **8-45**
- srcpAudit: GwCoordProto resolution **8-45**
- srcpAudit: GwCulpAddr resolution **8-45**
- srcpAudit: GwCulpPort resolution **8-46**

- srcpAudit: GwNumOfLines resolution **8-46**
- srcpAudit: GwSlotNum resolution **8-46**
- srcpAudit: GwSulpAddr resolution **8-46**
- srcpAudit: GwSulpPort resolution **8-47**
- srcpAudit: GwType resolution **8-47**
- srcpAudit: LineCoding resolution **8-47**
- srcpAudit: LineLoopback resolution **8-47**
- srcpAudit: LineSigProto resolution **8-47**
- srcpAudit: LineState resolution **8-48**
- SSN FAIL resolution **8-48**
- Standby Warm Start resolution **8-48**
- status monitoring **3-6**
- SUPPORT FAILED resolution **8-49**
- SwitchoverFail resolution **8-49**
- tools for troubleshooting **4-4**
- troubleshooting procedures **8-8**
- troubleshooting using alarms **8-2**
- understanding **3-7**
- viewing and searching **3-105**
- XE Rsrc Fail resolution **8-49**
- automatic congestion control *See* ACC
- automatic system log rotation **3-27**

B

- backing up system software
 - Cisco MGC software **3-28**
 - MMDB **3-33**
- BAMS
 - data dumper, configuring **A-5**
- bearer channels
 - administrative state, retrieving **3-59**
 - calls, stopping **8-91**
 - call state audit **8-91**
 - CIC mismatch **8-99**
 - CICs, blocking **3-58**
 - CICs, hung, manually resolving **8-88**
 - CICs, hung, resolving **8-87**
 - CICs, resetting **8-87**

- CICs, stuck, manually resolving **8-88**
- CICs, stuck, resolving **8-87**
- CICs, unblocking **8-86**
- CIC state mismatch, resolving **8-77**
- CIC states, querying **8-76**
- Cisco MGC, calls fail at **8-101**
- Cisco MGC, stopping calls on **8-91**
- continuity test, manual **8-96**
- continuity test, verifying settings **8-96**
- ISDN D-channel discrepancies **8-83**
- managing **3-55**
- media gateway, retrieving states held by **3-57**
- media gateway IP destination is OOS **8-98**
- media gateway IP links are OOS **8-98**
- MGCP media gateway, auditing **8-94**
- replication of calls, verifying **3-56**
- RLM, modifying timers **8-101**
- spans, stopping calls on **8-93**
- troubleshooting procedures **8-70**
- BLO messages, enabling **3-54**
- board layout, SLT **6-18**
- brackets
 - center mount, installing (figure) **6-8**
 - chassis, attaching to rack (figure) **6-9**
 - front panel, installing forward (figure) **6-7, 6-8**
 - identifying (figure) **6-7**
 - rear panel, installing forward (figure) **6-8**

C

- call detail records *See* CDRs
- call engine process **1-8**
- call instance component **1-8**
- calls
 - abnormal termination trace **8-110**
 - bearer channels, stopping on **8-91**
 - CICs, stopping on **8-94**
 - Cisco MGC, fails at **8-101**
 - Cisco MGC, stopping on **8-91**

- hung, diagnosing **8-109**
- media gateway, stopping on **8-92**
- signaling service, stopping on **8-92**
- spans, stopping calls on **8-93**
- state audit **8-91**
- trunk groups, stopping on **8-92**
- call trace
 - alternatives **8-108**
 - deleting files **8-106**
 - names of open traces, retrieving **8-105**
 - performing **8-103**
 - starting **8-103**
 - stopping **8-105**
 - tools for troubleshooting **4-4**
 - understanding **8-106**
 - viewing **3-117**
- call trace viewer
 - trace actions **3-117**
 - trace selection **8-105**
- Catalyst 5500 MSR
 - 1000 Mbps LED **7-3**
 - 100 Mbps LED **7-3**
 - AC power supply, handling (figure) **7-10**
 - AC power supply, installing **7-10**
 - AC power supply, removing **7-9**
 - AC power supply front panel (figure) **7-9**
 - active LED **7-2**
 - chassis fan assembly (figure) **7-16**
 - chassis fan assembly, removing and replacing **7-15**
 - command line interface **C-2**
 - command line interface, local access **C-3**
 - command line interface, remote access **C-3**
 - components, replacing **7-5**
 - DC power supply, CO ground (figure) **7-12**
 - DC power supply, connectors (figure) **7-15**
 - DC power supply, front panel (figure) **7-12**
 - DC power supply, handling (figure) **7-13**
 - DC power supply, installing **7-13**
 - DC power supply, removing **7-11**
 - ejector levers, using (figure) **7-6**
 - equipment status, checking **7-1**
 - Fast Ethernet switching module LEDs (figure) **7-4**
 - flash memory card, locating write-protection switch (figure) **7-8**
 - flash memory cards, using with supervisor engine **7-7**
 - LEDs **7-1**
 - LEDs, Ethernet switching module (figure) **7-3**
 - LEDs, Ethernet switching module (table) **7-3**
 - LEDs, Fast Ethernet switching module (figure) **7-4**
 - LEDs, Fast Ethernet switching module (table) **7-4**
 - LEDs, route switch module **7-4**
 - LEDs, supervisor engine III and uplink module (table) **7-2**
 - modules, avoiding problems when inserting or removing **7-6**
 - PCMCIA card, replacement **7-7**
 - PCMCIA card installation **7-7**
 - power down procedure **2-5**
 - power on procedure **2-3**
 - power supply, removing and replacing **7-8**
 - PS1 LED **7-2**
 - route switch module (table) **7-5**
 - route switch module LEDs (figure) **7-4**
 - slot 1 LED **7-3**
 - slot 2 LED **7-3**
 - status, checking **7-5**
 - status LED **7-3**
 - supervisor engine, removing **7-6**
 - supervisor engine, replacing **7-7**
 - supervisor engine III front panel (figure) **7-2**
 - supervisor engine module LEDs **7-2**
 - switch load LED **7-2**
 - system status LED **7-2**
 - tools, removal and replacement procedures **7-6**
 - virtual LANs **C-1**
 - virtual pathways and ISLs, troubleshooting **C-3**
- caution
 - chassis-cover replacement **6-21**
 - DIMM handling **6-18**

- flash memory SIMM replacement **6-20**
 - hot swapping not supported **6-14**
 - SIMM handling **6-20**
 - CDRs
 - data dumper, configuring **A-2**
 - data dumper, configuring to support BAMS **A-5**
 - dumper sink log file parameters (table) **A-3**
 - not being generated **8-123**
 - searching **3-110**
 - viewer, configuring **3-108**
 - CDR viewer
 - config tab window (figure) **3-108**
 - configuring
 - ConnHost tab window (figure) **3-109**
 - query tab window (figure) **3-111**
 - using **3-107**
 - CICs
 - administrative state, retrieving **3-62**
 - administrative state, setting **8-75**
 - blocking **3-58**
 - calls, stopping **8-94**
 - call state audit **8-91**
 - call states (table) **3-15**
 - circuit block types (table) **3-16**
 - hung, manually resolving **8-88**
 - hung, resolving **8-87**
 - media gateway states (table) **3-15**
 - mismatch **8-99**
 - primary service states (table) **3-14**
 - querying states **8-76**
 - resetting **8-87**
 - resolving state mismatch **8-77**
 - states, understanding **3-14**
 - states, verifying **3-13**
 - stuck, manually resolving **8-88**
 - stuck, resolving **8-87**
 - unblocking **8-86**
 - Cisco MGC node connectivity (figure) **1-3**
 - components
 - data, retrieving **3-87**
 - type data, retrieving **3-88**
 - config-lib viewer window (figure) **3-113**
 - config tab window (figure) **3-108**
 - configuration data
 - backup files, listing **8-122**
 - backup files, restoring **8-122**
 - local tape drive, restoring from **8-118**
 - remote machine, restoring from **8-119**
 - configuration parameters, retrieving **3-89**
 - configurations, administering **3-113**
 - configuration tables
 - alarm categories **3-87**
 - components **3-87**
 - component types **3-88**
 - data, retrieving **3-87**
 - default configuration parameters **3-89**
 - measurement categories **3-88**
 - retrieving **3-89**
 - services **3-88**
 - ConnHost tab window (figure) **3-109**
 - console port
 - baud rate settings, SLT **6-12**
 - connecting (figure) **6-12**
 - connecting devices to **6-12**
 - continuity test
 - manual **8-96**
 - settings, verifying **8-96**
 - cover
 - replacement caution **6-21**
-
- ## D
- daily tasks
 - alarm status monitoring **3-6**
 - CIC states, verifying **3-13**
 - CPU utilization level, verifying **3-19**
 - destinations, verifying the status of all **3-8**
 - disk space, verifying available **3-17**

- memory on the SLT, verifying available **3-23**
 - MML session, starting **3-2**
 - platform state, verifying **3-2**
 - processes, verifying **3-3**
 - processes, verifying the number of active **3-21**
 - RAM, verifying available **3-19**
 - SS7 routes, verifying state of all **3-10**
 - users, verifying the number of **3-22**
 - virtual memory, verifying available **3-17**
 - data dumper
 - BAMS, configuring to support **A-5**
 - configuring **A-2**
 - dumper sink log file parameters (table) **A-3**
 - DC power
 - connections (figure) **6-10**
 - specifications (table) **6-9**
 - supply, installing **6-9**
 - wiring **6-9**
 - DC power supply
 - CO ground (figure) **7-12**
 - connectors (figure) **7-15**
 - front panel (figure) **7-12**
 - handling (figure) **7-13**
 - installing **7-13**
 - removal and replacement **7-8**
 - removing **7-11**
 - debug commands
 - troubleshooting **4-7**
 - diagnostics log file, creating **8-8**
 - dial plan
 - backup **3-33**
 - proper loading, verifying **8-69**
 - provisioning **3-73**
 - restoring **8-121**
 - translation, verifying **3-118**
 - translation configuration data, viewing **3-123**
 - verifying **3-118**
 - DIMM
 - handling caution **6-18**
 - disk monitor **3-24**
 - configuring **3-25**
 - disk space, verifying amount available **3-17**
 - DPC primary link service states (table) **3-9**
 - DPCs
 - primary service states (table) **3-9**
 - state information **3-9**
 - verifying status **3-8**
 - dynamic reconfiguration
 - invoking **3-65**
 - preconditions (table) **3-66**
 - understanding **3-66**
-
- ## E
- EIA/TIA-232
 - console port connections **6-12**
 - element management subsystem **1-5**
 - equipment status, checking **5-1**
 - Ethernet connections, Cisco MGC node **1-2**
 - execution environment process shell **1-7**
-
- ## F
- failover daemon **1-6**
 - failure
 - Cisco MGC **8-2**
 - operating system **8-2**
 - SLT **8-2**
 - fan
 - LED, supervisor engine **7-2**
 - removal and replacement **7-15**
 - fault tolerance subsystem **1-6**
 - file options viewer window (figure) **3-125**
 - flash memory
 - PCMCIA card replacement **7-7**
 - SIMMs, replacing **6-19**

G

group service reset messages *See* GSR messages

GSR messages

enabling **3-55**

H

hardware maintenance procedures

SLT **6-15**

hardware shutdown

Cisco MGC **2-4**

I

I/O card

MTP2 timers, verifying **8-62**

I/O cards

MTP2 timers, modifying **8-66**

input/output system **1-5**

installation

DC power connections (figure) **6-10**

DC power supply **6-9**

DC power supply specifications (table) **6-9**

network connections **6-11**

SLT rack-mount **6-6**

system-code SIMMs, SLT **6-19**

tools, parts, and equipment required for SLT **6-6**

wiring DC power supply **6-9**

installiation

PCMCIA card, Catalyst 5500 MSR **7-7**

interface numbering, SLT **6-12**

IOCCs **1-5**

IOCMs **1-5**

IP FAS, enabling BLO/UBL messages **3-54**

J

Japanese SS7

signaling link tests **8-67**

signaling route tests **8-68**

L

LEDs

1000 Mbps **7-3**

100 Mbps **7-3**

active **7-2**

Catalyst 5500 MSR Ethernet switching module
(figure) **7-3**

Catalyst 5500 MSR Ethernet switching module
(table) **7-3**

Catalyst 5500 MSR fan **7-2**

Catalyst 5500 MSR Fast Ethernet switching module
(figure) **7-4**

Catalyst 5500 MSR Fast Ethernet switching module
(table) **7-4**

Catalyst 5500 MSR link **7-3**

Catalyst 5500 MSR route switch module **7-4**

Catalyst 5500 MSR slot 1 **7-3**

Catalyst 5500 MSR slot 2 **7-3**

Catalyst 5500 MSR status **7-3**

Catalyst 5500 MSR supervisor engine III and uplink
module (table) **7-2**

Catalyst 5500 MSR supervisor engine module **7-2**

Catalyst 5500 MSR switch load **7-2**

Catalyst 5500 MSR system status **7-2**

Cisco Catalyst 5500 MSR **7-1**

Fast Ethernet switching module (figure) **7-4**

PS1 **7-2**

reading **4-1**

route switch module **7-5**

route switch module (figure) **7-4**

SLT **6-2**

SLT front panel (figure) **6-2**

SLT front panel (table) **6-2**

SLT multiflex trunk interface card (table) **6-4**

SLT rear panel (figure) **6-3**

SLT rear panel (table) **6-3**

SLT serial WAN interface cards (figure) **6-4**

SLT T1 and E1 multiflex trunk interface cards (figure) **6-4**

SLT virtual WAN interface cards **6-4**

SLT WAN interface cards **6-3**

Sun Enterprise 450 **5-2**

Sun Netras **5-1**

link

- service state, setting **8-60**

links

- bouncing, resolving **8-56**
- measurements, retrieving **3-91**

linkset

- service state, retrieving **3-51**
- service state, setting **8-60**

linksets

- measurements, retrieving **3-91**

local subsystem number *See* LSSN

logs

- diagnostics file, creating **8-8**
- file types **A-1**
- messages, understanding **8-6**
- rotation, automatic **3-27**
- rotation, manual **3-27**
- searching **3-115**
- tools for troubleshooting **4-4**
- troubleshooting **8-4**
- understanding **A-1**
- viewing **8-4**

log viewer

- searching **3-115**
- using **3-114**
- window (figure) **3-115**

LSSN

- service state, setting **8-61**

M

maintenance

- checking Cisco MGC status **5-1**
- components **5-3**
- GUI NMS, using **4-1**
- LEDs, reading **4-1**
- LEDs, Sun Enterprise 450 LEDs **5-2**
- LEDs, Sun Enterprise 450 platform (table) **5-2**
- LEDs, Sun Netras **5-1**
- SLT **6-15**
- software, backing up **3-28**
- status queries, issuing **4-1**
- strategy overview **4-1**
- technical support staff **5-3**

maximum ACL mapping values (table) **3-79**

meas record view tab window (figure) **3-104**

measurements

- ANSI ISUP measurements (table) **D-13**
- archived, field descriptions (table) **A-7**
- clearing **3-91**
- data dumper, configuring **A-2**
- dumper sink log file parameters (table) **A-3**
- ITU measurements (table) **D-1**
- links or linksets, retrieving **3-91**
- managing **3-90**
- not being generated **8-123**
- retrieving **3-90**
- SS7 signaling point, retrieving **3-93**
- viewing and searching **3-104**

measurements

- category data, retrieving **3-88**

media gateway

- administrative state, retrieving **3-60**
- administrative state, setting **8-71**
- calls, stopping **8-92**
- MGCP, auditing **8-94**

memory, SLT system-code SIMMs (flash memory) **6-19**

MGC backup viewer window (figure) **3-125**

MGC restore viewer window (figure) **3-126**

MGC toolbar window (figure) **3-103**

MGC viewer toolkit

alarm and measurement viewer **3-103**

CDR viewer **3-107**

config-lib viewer **3-113**

file options viewer **3-124**

log viewer **3-114**

MGC backup viewer **3-125**

MGC restore viewer **3-125**

MGC toolbar window (figure) **3-103**

toolbar, launching **3-103**

trace viewer **3-117**

translation verification viewer **3-118**

MML

as a tool for troubleshooting **4-4**

commands, displaying information about **3-41**

commands, displaying previously entered **3-40**

commands, reentering previously entered **3-46**

session, ending **3-47**

session, managing **3-39**

session, retrieving active **3-47**

session, starting **3-2**

MML terminal **1-5**

modem

connecting **6-11**

MTP1 communication, identifying problems **B-11**

MTP1 communication, solving problems **B-11**

MTP2 communication, identifying problems **B-12**

MTP2 communication, solving problems **B-12**

MTP2 timers

I/O card, verifying **8-62**

I/O cards, modifying **8-66**

SLTs, modifying **8-65**

verifying on an SLT **8-62**

MTP3 timers

modifying **8-66**

verifying **8-63**

MTP timers

settings, modifying **8-65**

settings, verifying **8-61**

N

network management tools

Cisco Media Gateway Controller Node Manager **4-6**

Cisco WAN Manager **4-5**

CiscoWorks2000 **4-5**

P

periodic maintenance procedures

automatic backup operation, deleting **3-38**

automatic backup operation, listing **3-37**

automatic backup operation, scheduling **3-35**

backing up system software **3-28**

backup history, listing **3-39**

disk space, automatic monitoring **3-24**

full backup operation, storing on a local tape **3-29**

full backup operation, storing on a remote machine **3-30**

log rotation, automatic **3-27**

manual backup operation **3-34**

MMDB backup **3-33**

partial backup operation, storing on a local tape **3-29**

partial backup operation, storing on a remote machine **3-32**

periodic maintenance procedures

disk monitor, configuring **3-25**

platform management

manual switchover, performing **3-80**

patch level, verifying for the Cisco MGC **3-85**

switchover, understanding **3-82**

switchover, verifying successful completion **3-82**

platform management

configuration table data, retrieving **3-87**

processes, retrieving the logging level **3-89**

platform state, verifying **3-2**

platform troubleshooting

- backup files, listing **8-122**
- backup files, restoring **8-122**
- CDRs, not being generated **8-123**
- Cisco MGC, recovering from a failure **8-115**
- data, restoring from a local tape drive **8-118**
- data, restoring from a remote machine **8-119**
- deleting files **8-112**
- dial plan, restoring a **8-121**
- measurements, not being generated **8-123**
- peer, resolving failed connection to **8-125**
- properties, rebooting to modify **8-124**
- replication, verifying configuration **8-123**
- software, rebooting to modify configuration parameters **8-125**
- stored configuration data, restoring **8-117**
- switchover failure, recovering **8-113**
- point codes
 - state, retrieving **3-51**
- power down procedure
 - Cisco MGC **2-4**
- power on procedure
 - Cisco MGC **2-2**
- power supply
 - Catalyst 5500 MSR, removal and replacement **7-8**
- Preface
 - Document Organization **x**
- processes
 - logging level, changing **8-6**
 - logging level, lowest possible (table) **8-6**
 - logging level, retrieving **3-89**
 - process manager, controlled by (table) **3-5**
 - understanding **3-4**
 - verifying **3-3**
 - verifying the number of active **3-21**
- properties
 - rebooting to modify **8-124**
- provisioning
 - changes, saving and activating **3-64**
 - data, exporting **3-74**

- data, retrieving **3-67**
- data, retrieving for all components **3-69**
- data, retrieving for all components of a particular type **3-70**
- data, retrieving for an individual component **3-68**
- data, retrieving for the current session **3-71**
- data, retrieving supported signaling protocols **3-71**
- dial plan **3-73**
- dynamic reconfiguration, invoking **3-65**
- managing ACC **3-75**
- maximum ACL value, modifying **3-79**
- overload level, retrieving **3-80**
- session, ending without activating changes **3-65**
- session, starting **3-63**
- provisioning, dynamic reconfiguration, understanding **3-66**

Q

- query tab window (figure) **3-111**

R

- rack equipment
 - SLT installation **6-6**
- RAM, verifying available amount **3-19**
- regular operations
 - bearer channels, managing **3-55**
 - Cisco MGC, provisioning **3-63**
 - Cisco MGC platform, managing **3-80**
 - Cisco MGC viewer toolkit **3-102**
 - measurements, managing **3-90**
 - MML session, managing **3-39**
 - signaling channels, managing **3-47**
- replication
 - configuration, verifying **8-123**
- replication of calls **3-56**
- replicator **1-6**
- restore

- backup files, listing **8-122**
- backup files, restoring **8-122**
- local tape drive **8-118**
- remote machine **8-119**
- RLM
 - timers, modifying **8-101**
- rollover cable (figure) **6-11**
- rollover cable, identifying **6-11**

S

- services, retrieving **3-88**
- show commands
 - troubleshooting **4-7**
- signaling channels
 - attributes, retrieving **3-48**
 - configuration errors **8-54**
 - enabling BLO/UBL messages **3-54**
 - GSR messages, enabling
 - incomplete signaling **8-54**
 - linkset, retrieving service state **3-51**
 - managing **3-47**
 - physical layer failures **8-54**
 - point codes, retrieving the state of **3-51**
 - primary service states (table) **3-49**
 - service state, setting **8-58**
 - service states, changing **8-55**
 - signaling destination service states, retrieving **3-50**
 - SS7 link is out-of-service **8-51**
 - SS7 loadsharing malfunction **8-52**
 - state of all LSSNs, retrieving **3-53**
 - state of all RSSNs, retrieving **3-53**
 - state of SS7 routes, retrieving **3-52**
 - supporting entity failures **8-54**
 - TCAP transactions, clearing **3-54**
 - TCAP transactions, retrieving **3-53**
 - understanding **3-48**
- signaling destinations
 - configuration errors **8-57**
 - links, resolving bouncing **8-56**
 - service state, setting **8-59**
 - traffic restart **8-57**
- signaling link terminal *See* SLT
- signaling point codes
 - service state, setting **8-60**
- signaling service
 - administrative state, retrieving **3-60**
 - administrative state, setting **8-73**
 - calls, stopping on **8-92**
- SIMM
 - handling caution **6-20**
- SIMMs
 - replacing, SLT **6-19**
 - SLT system-code (flash) **6-19**
 - SLT system-code, replacing **6-19**
 - tools, required for replacement **6-20**
- SLT
 - backing up software **6-19**
 - baud rate, console terminal **6-12**
 - board layout **6-18**
 - boot and system images, recovering **6-22**
 - bracket, center mount installation (figure) **6-8**
 - bracket, front panel installation forward (figure) **6-7, 6-8**
 - bracket, rear panel installation forward (figure) **6-8**
 - brackets, identifying (figure) **6-7**
 - chassis
 - removing cover, (figure) **6-17**
 - chassis, attaching to rack (figure) **6-9**
 - chassis, closing **6-21**
 - chassis, holding for cover removal (figure) **6-17**
 - chassis, opening **6-17**
 - chassis, replacing cover **6-21**
 - Cisco MGC communications, troubleshooting **B-13**
 - components, replacing **6-13**
 - connecting console terminal and modem **6-11**
 - connecting DC power supply **6-9**
 - connecting to a console port (figure) **6-12**
 - connection management **B-3**

- console port, connecting to **6-12**
- cover, replacing **6-21**
- data link layer, MTP2 communication problem (figure) **B-12**
- DC power connections (figure) **6-10**
- DC power supply specifications (table) **6-9**
- debug outputs, probable causes, and recovery actions (table) **B-6, B-8**
- DRAM DIMM, removing/replacing (figure) **6-19**
- equipment status, checking **6-2**
- error messages (table) **B-15**
- Ethernet connectivity, identifying problems **B-14**
- flash memory SIMM, replacing **6-20**
- front-panel LEDs (figure) **6-2**
- hardware and I/O signaling (figure) **B-1**
- interface numbering **6-12**
- IP communication, identifying problems **B-14**
- IP signaling backhaul **B-2**
- layout, system card (figure) **6-18**
- LEDs **6-2**
- LEDs, front-panel (table) **6-2**
- LEDs, multiflex trunk interface card (table) **6-4**
- LEDs, rear-panel (table) **6-3**
- LEDs, serial WAN interface card (figure) **6-4**
- LEDs, virtual WAN interface card **6-4**
- LEDs, WAN interface card **6-3**
- links to STPs, troubleshooting **B-10**
- maintenance procedures **6-15**
- memory, verifying amount available **3-23**
- MTP1 communication problems **B-11**
- MTP1 communication problems, identifying **B-11**
- MTP1 communication problems, solving **B-11**
- MTP2 communication problems **B-12**
- MTP2 communication problems, identifying **B-12**
- MTP2 communication problems, solving **B-12**
- MTP2 timers, modifying **8-65**
- MTP2 timers, verifying **8-62**
- MTP3 and higher layers, identifying problems **B-13**
- MTP3 and higher layers, solving problems **B-14**
- MTP3 and higher layer SS7 protocol processing (figure) **B-13**
- network connections **6-11**
- opening the chassis **6-16**
- physical layer, MTP1 communication problems (figure) **B-11**
- power down procedure **2-5**
- power on procedure **2-3**
- rack installation **6-9**
- rack-mounting **6-6**
- rear-panel LEDs (figure) **6-3**
- removing **6-5**
- replacing **6-6**
- rollover cable (figure) **6-11**
- rollover cable, identifying **6-11**
- SIMMs, replacing **6-19**
- software, installation **6-13**
- system card layout (figure) **6-18**
- system-code SIMM, removing/replacing (figure) **6-21**
- system-code SIMMs, replacing **6-19**
- system status, checking **6-4**
- tools, required **6-14**
- tools required for DRAM SIMM replacement **6-17**
- tools required for installation **6-6**
- WAN interface card, installation **6-14**
- WAN interface card chassis slot locations (figure) **6-13**
- WIC-2T dual port serial WAN interface card (figure) **6-14**
- wiring DC power supply **6-9**
- SLTLEDs,
 - T1 and E1 multiflex trunk interface card (figure) **6-4**
- SNMP terminal **1-5**
- software
 - automatic backup operation, deleting **3-38**
 - automatic backup operation, listing **3-37**
 - automatic backup operation, scheduling **3-35**
 - backing up SLT before replacing SIMMs **6-19**
 - backup files, listing **8-122**
 - backup files, restoring **8-122**
 - backup history, listing **3-39**

- directory structure **1-10**
- directory structure (table) **1-10**
- full backup operation
 - storing on a remote machine **3-30**
- full backup operation, storing on a local tape **3-29**
- manual backup operation **3-34**
- partial backup operation, storing on a local tape **3-29**
- partial backup operation, storing on a remote machine **3-32**
- restore from a local tape drive **8-118, 8-122**
- restore from a remote machine **8-119**
- restore MMDB **8-121**
- SLT boot and system images, recovering **6-22**
- SLT installation **6-13**
- SLT system-code SIMMs, replacing **6-19**
- upgrades **5-3**
- verifying version **3-2**
- software architecture
 - call engine process **1-8**
 - call instance component **1-8**
 - Cisco MGC software system diagram (figure) **1-4**
 - element management subsystem **1-5**
 - execution environment process shell **1-7**
 - fault tolerance subsystem **1-6**
 - input/output subsystem **1-5**
- software shutdown
 - Cisco MGC **2-4**
- software startup
 - Cisco MGC **2-2**
- spans
 - administrative state, retrieving **3-61**
 - administrative state, setting **8-73**
- SRCP audit alarm
 - resolving **8-97**
- SS7 network
 - troubleshooting **8-50**
- SS7 routes
 - primary service states (table) **3-12**
 - state, verifying **3-10**

- state information, understanding **3-11**
- SS7 signaling point, retrieving measurements **3-93**
- SS7 troubleshooting
 - signaling destination OOS, resolving **8-57**
 - signaling destination unavailable, resolving **8-58**
 - signaling route OOS, resolving **8-57**
- switchover
 - checkpointing **3-84**
 - circuit auditing **3-84**
 - completion, verifying **3-82**
 - failover daemon **3-83**
 - failure, recovering from **8-113**
 - fault-tolerant components **3-82**
 - manual, performing **3-80**
 - understanding **3-82**

T

- TCAP trace **8-111**
- TCAP transactions
 - retrieving **3-53**
- TCAP transactions, clearing **3-54**
- technical support staff
 - personnel, skill level **5-3**
 - software troubleshooting tools **5-3**
- trace viewer
 - using **3-117**
 - window (figure) **3-117, 3-118**
- traffic channel and CIC primary link service states (table) **3-14**
- traffic channels
 - call states (table) **3-15**
 - circuit block types (table) **3-16**
 - media gateway states (table) **3-15**
 - primary service states (table) **3-14**
 - states, understanding **3-14**
- translation verification viewer
 - config tab window (figure) **3-124**
 - dial plan, verifying **3-118**

dial plan translation configuration data, viewing **3-123**

dial plan translation tab window (figure) **3-119**

troubleshooting

- alarms, using **8-2**
- bearer channel connection procedures **8-70**
- bit error rate testers **4-10**
- block error rate testers **4-10**
- breakout boxes **4-10**
- cable testers **4-9**
- debug commands **4-7**
- digital multimeters **4-9**
- fox boxes **4-10**
- general problem-solving model (figure) **4-2, 4-3**
- network analyzers **4-10**
- network monitors **4-10**
- optical time domain reflectometers **4-10**
- ping command **4-8**
- show commands **4-7**
- signaling destination OOS, resolving **8-57**
- signaling destination unavailable, resolving **8-58**
- signaling route OOS, resolving **8-57**
- SLT diagnostic commands **4-6**
- SS7 network procedures **8-58**
- SS7 network related problems **8-50**
- strategy overview **4-2**
- third-party tools **4-9**
- time domain reflectometers **4-10**
- tools **4-4**
- trace command **4-8**
- volt-ohm meters **4-9**

trunk group

- administrative state, retrieving **3-60**
- administrative state, setting **8-72**

trunk groups

- calls, stopping on **8-92**

users, verifying the number of **3-22**

V

virtual memory, verifying available amount **3-17**

W

WAN interface cards

- slot filler panel (figure) **6-15**

- SLT chassis slot locations (figure) **6-13**

- two-slot network module, installation in a **6-14**

warning

- DC power connection, SLT **6-15**

- equipment, holding with both hands, Catalyst 5500
MSR **7-12, 7-14**

- power, turning off, Catalyst 5500 MSR **7-11, 7-13**

- power supply bay high voltage, Catalyst 5500
MSR **7-13, 7-14**

U

UBL messages, enabling **3-54**