



Cisco Integrated Network Solutions Operations, Maintenance, and Troubleshooting Guide

Corporate Headquarters

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

Customer Order Number:
Text Part Number: OL-1519-01



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, the Cisco *Powered* Network mark, the Cisco Systems Verified logo, Cisco Unity, Follow Me Browsing, FormShare, Internet Quotient, iQ Breakthrough, iQ Expertise, iQ FastTrack, the iQ Logo, iQ Net Readiness Scorecard, Networking Academy, ScriptShare, SMARTnet, TransPath, and Voice LAN are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, Discover All That's Possible, The Fastest Way to Increase Your Internet Quotient, 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, IOS, IP/TV, LightStream, MGX, MICA, the Networkers logo, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, RateMUX, Registrar, SlideCast, StrataView Plus, Stratm, SwitchProbe, TeleRouter, 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. (0203R)

Cisco Integrated Network Solutions Operations, Maintenance, and Troubleshooting Guide

Copyright © 2002, Cisco Systems, Inc.

All rights reserved.



CONTENTS

Preface **xxix**

Document and Solution Release	xxx
Audience	xxx
Scope	xxx
Document Organization	xxxii
Related Documents	xxxv
Viewing Online Documents in Your Browser	xxxv
Document Conventions	xxxv
Obtaining Documentation	xxxvii
World Wide Web	xxxvii
Documentation CD-ROM	xxxvii
Ordering Documentation	xxxvii
Documentation Feedback	xxxvii
Obtaining Technical Assistance	xxxviii
Cisco.com	xxxviii
Technical Assistance Center	xxxviii
Contacting TAC by Using the Cisco TAC Website	xxxviii
Contacting TAC by Telephone	xxxix

CHAPTER 1

How to Use This Guide	1
Overview	1
Prerequisites	2
Cisco ASAP Solution References	2
PSTN Gateway Solutions References	2
Operations and Maintenance Tasks: At a Glance	3
Regularly Scheduled Tasks	3
General Operations and Maintenance Guidelines	4
As-Needed Tasks	7
Resource and Network Performance Management	14
Resource Management	14
Network Management	15
Management Tools	15
Troubleshooting and Trouble Clearing Tasks: At a Glance	17

CHAPTER 2

Managing Network Elements and Dial Plans: Using Cisco Voice Manager 1

- Introduction** 1
 - Target Platforms** 1
 - References** 1
 - Task Summary** 2
 - Managing Network Elements** 2
 - Managing Dial Plans** 2
 - Managing Voice Ports** 2
- Creating, Modifying, and Deleting a UG Group** 3
 - Description** 3
 - Reference** 3
 - Procedure** 3
 - Notes** 3
- Adding, Modifying, and Deleting a Gatekeeper** 4
 - Description** 4
 - Reference** 4
 - Procedure** 4
 - Notes** 4
- Creating, Modifying, and Deleting a Local Zone on a GK** 5
 - Description** 5
 - Reference** 5
 - Procedure** 5
 - Notes** 5
- Creating, Modifying, and Deleting a Remote Zone on a GK** 6
 - Description** 6
 - Reference** 6
 - Procedure** 6
 - Notes** 6
- Adding, Modifying, Locating, and Deleting a UG** 7
 - Description** 7
 - Reference** 7
 - Procedure** 7
 - Notes** 7
- Synchronizing Devices** 8
 - Description** 8
 - Reference** 8
 - Procedure** 8
- Moving a UG** 9
 - Description** 9

Reference	9
Procedure	9
Scheduling Tasks	10
Description	10
Reference	10
Procedure	10
Creating, Modifying, and Deleting a Local Dial Plan	11
Description	11
Reference	11
Procedure	11
Notes	11
Creating, Modifying, and Deleting a Network Dial Plan	12
Description	12
Reference	12
Procedure	12
Notes	12
Modifying FXO, FXS, E&M, and ISDN Voice Ports	13
Description	13
Reference	13
Procedure	13
Notes	13

CHAPTER 3**Managing Resources and Dial Services:****Using Cisco RPMS 1**

Introduction	1
Target Platforms	2
References	2
Task Summary	2
Cisco RPMS Server Administration	2
Configuring Port Management	2
Configuring Service Level Agreements	3
Configuring Fault Tolerance	3
Reporting and Accounting	3

Cisco RPMS Server Administration:**Configuring Cisco RPMS Settings 4**

Description	4
Reference	4
Procedure	4
Notes	4

Cisco RPMS Server Administration:	
Configuring Administrators and Administrators' Privileges	5
Description	5
Reference	5
Procedure	5
Notes	5
Cisco RPMS Server Administration:	
Configuring Alert Notifications and Logging	6
Description	6
Reference	6
Procedure	6
Notes	6
Cisco RPMS Server Administration:	
Configuring RADIUS Vendors and VSAs	7
Description	7
Reference	7
Procedure	7
Notes	8
Cisco RPMS Server Administration:	
Communicating with Universal Gateways	9
Description	9
Reference	9
Procedure	9
Notes	9
Cisco RPMS Server Administration:	
Configuring AAA Servers	10
Description	10
Reference	10
Procedure	10
Notes	11
Cisco RPMS Server Administration:	
Configuring SNMP Management	12
Description	12
Reference	12
Procedure	12
Notes	12
Cisco RPMS Server Administration:	
Resetting Counters	13
Description	13
Reference	13

Procedure	13
Notes	13
Cisco RPMS Server Administration:	
Managing the Universal Gateway Heartbeat	14
Description	14
Reference	14
Procedure	14
Notes	14
Cisco RPMS Server Administration:	
Performing Cisco RPMS Administration Tasks	15
Description	15
Reference	15
Procedure	15
Notes	15
Configuring Port Management:	
Configuring DNIS Groups	16
Description	16
Reference	16
Procedures	16
Notes	17
Configuring Port Management:	
Configuring Trunk Groups	18
Description	18
Reference	18
Procedures	18
Notes	18
Configuring Port Management:	
Understanding Call Types	19
Description	19
Reference	19
Procedure	19
Notes	20
Configuring Service Level Agreements:	
Configuring Customer Profiles	21
Description	21
Reference	21
Procedure	21
Notes	21
Configuring Service Level Agreements:	
Configuring Call Discrimination	22

Description	22
Reference	22
Procedure	22
Notes	23
Configuring Service Level Agreements:	
Configuring VPDN Services	24
Description	24
Reference	24
Procedure	24
Notes	25
Configuring Service Level Agreements:	
Creating Overflow Pools	26
Description	26
Reference	26
Procedures	26
Notes	27
Configuring Fault Tolerance:	
Configuring Cisco RPMS Fault Tolerance	28
Description	28
Reference	28
Procedure	28
Notes	29
Configuring Fault Tolerance:	
Configuring Fault Tolerance in Cisco RPMS Servers	30
Description	30
Reference	30
Procedure	30
Notes	30
Configuring Fault Tolerance:	
Configuring Tolerance to an AAA Server Failure	31
Description	31
Reference	31
Procedure	31
Notes	32
Reporting and Accounting:	
Using Cisco RPMS Reporting	33
Description	33
Reference	33
Procedure	33
Notes	33

Reporting and Accounting:	
Generating Report Types	34
Description	34
Reference	34
Procedure	34
Notes	35
Reporting and Accounting:	
Configuring Accounting	36
Description	36
Reference	36
Procedure	36
Notes	36

CHAPTER 4

Managing Network Objects:	
Using Cisco UGM	1
Introduction	1
Target Platforms	1
References	2
Task Summary	2
Deploying and Discovering Network Objects	3
Description	3
Reference	3
Procedure	3
Managing and Exporting Inventory Data	4
Description	4
Reference	4
Procedure	4
Managing Redundancy and High Availability	5
Description	5
Reference	5
Procedure	5
Configuring Managed Devices	6
Description	6
Reference	6
Procedure	6
Managing Images and Scheduling Actions	8
Description	8
Reference	8
Procedure	8

- Configuring the Administrative State of Objects** 9
 - Description** 9
 - Reference** 9
 - Procedure** 9
- Managing Security on Cisco UGM-Managed Devices** 10
 - Description** 10
 - Reference** 10
 - Procedure** 10
- Managing Device Performance** 11
 - Description** 11
 - Reference** 11
 - Procedure** 11
- Managing Faults** 12
 - Description** 12
 - Reference** 12
 - Procedure** 12
- Managing Presence Polling and Loss of Communication** 13
 - Description** 13
 - Reference** 13
 - Procedure** 13

CHAPTER 5

**Managing SS7 Signaling Components:
Using Cisco MGC Node Manager** 1

- Introduction** 1
- Target Platforms** 2
- References** 2
 - Cisco MGC Release 7** 2
 - Cisco MGC Release 9** 2
- Task Summary** 2
 - Configuring Devices for Management** 2
 - Managing Security** 2
 - Deploying a Site, Object, or Network** 2
 - Monitoring Network Performance** 3
 - Managing Traps and Events** 3
 - Viewing Information about Network Devices** 3
 - Event Messages and Problem Correction** 3
- Configuring Network Devices for Management** 4
 - Description** 4
 - Reference** 4

Procedure	4
Setting Up Cisco MNM Security	5
Description	5
Reference	5
Procedure	5
Deployment:	
Using a Seed File to Deploy a Cisco MGC Network	6
Description	6
Reference	6
Procedure	6
Notes	6
Deployment:	
Manually Deploying a Site, Object, or Network	7
Description	7
Reference	7
Procedure	7
Notes	8
Discovery:	
Discovering a Cisco SLT, LAN Switch, Cisco MGC Host, or BAMS	9
Description	9
Reference	9
Procedure	9
Managing Software Images and Configurations	10
Description	10
Reference	10
Procedure	10
Monitoring Network Performance:	
Setting Polling Parameters	11
Description	11
Reference	11
Procedure	11
Notes	12
Monitoring Network Performance:	
Viewing and Managing Performance Data	13
Description	13
Reference	13
Procedure	13
Notes	14
Managing Traps and Events:	
Managing, Clearing, and Forwarding Traps	15

Description	15
Reference	15
Procedure	15
Notes	16
Managing Traps and Events:	
Managing Events	17
Description	17
Reference	17
Procedure	17
Notes	18
Managing Traps and Events:	
Miscellaneous Tasks	19
Description	19
Reference	19
Procedure	19
Notes	20
Managing Traps and Events:	
Setting How Long Alarms are Stored	21
Description	21
Reference	21
Procedure	21
Notes	21
Viewing Information about Network Devices:	
Available Information	22
Description	22
Reference	22
Procedure	22
Notes	23
Viewing Information about Network Devices:	
Using Diagnostic Tools	24
Description	24
Reference	24
Procedure	24
Notes	25
Event Messages: BAMS, Cisco MGC, and Cisco MNM	26
Description	26
Reference	26
Procedure	26

CHAPTER 6**Operating and Maintaining Cisco Devices:****Using Cisco Info Center 1****Introduction 1****Target Platforms 2****References 2****Task Summary 2****Installing and Configuring Relevant Components of CIC 2****Operating and Maintaining CIC Components 3****Managing Events and Traps Using CIC 3****Troubleshooting 3****Manually Starting and Stopping CIC Components 4****Description 4****Reference 4****Procedure 4****Starting and Stopping the Cisco Info Server 5****Description 5****Reference 5****Procedure 5****Modifying Configurations Using the Configuration Manager 6****Description 6****Reference 6****Procedure 6****Configuring Remote Processes Using Process Control 7****Description 7****Reference 7****Procedure 7****Creating a New Cisco Info Server 8****Description 8****Reference 8****Procedure 8****Using the Event List to Display Alerts 9****Description 9****Reference 9****Procedure 9****Managing the Cisco Info Server Using CLI Options 10****Description 10****Reference 10****Procedure 10****Creating and Editing the Interfaces File 12**

- Description** 12
- Reference** 12
- Procedure** 12
- Managing Objects Using the Objective View** 13
 - Description** 13
 - Reference** 13
 - Procedure** 13
- Managing User Access** 14
 - Description** 14
 - Reference** 14
 - Procedure** 14
- Creating, Editing, and Managing Filters Using the Filter Builder** 15
 - Description** 15
 - Reference** 15
 - Procedure** 15
- Creating, Editing, and Managing Views Using View Builder** 16
 - Description** 16
 - Reference** 16
 - Procedure** 16
- Troubleshooting: Using CIC Diagnostic Tools** 17
 - Description** 17
 - Reference** 17
 - Procedure** 17

CHAPTER 7

- Operating and Maintaining the Cisco Access Registrar** 1
 - Introduction** 1
 - Target Platforms** 1
 - References** 2
 - Task Summary** 2
 - Installing and Upgrading the Cisco AR** 2
 - Configuring a Basic Site** 2
 - Making Custom Configurations** 2
 - Performing Maintenance and Management Tasks** 3
 - Configuring Clients** 4
 - Description** 4
 - Reference** 4
 - Procedure** 4
 - Notes** 4

Configuring Profiles	5
Description	5
Reference	5
Procedure	5
Validating Configurations	6
Description	6
Reference	6
Procedure	6
Notes	6
Configuring Groups	7
Description	7
Reference	7
Procedure	7
Notes	7
Configuring Multiple UserLists	8
Description	8
Reference	8
Procedure	8
Notes	8
Configuring a Remote Server	9
Description	9
Reference	9
Procedure	9
Notes	9
Configuring Session Management	10
Description	10
Reference	10
Procedure	10
Checking the AR Server	11
Description	11
Reference	11
Procedure	11
Logging in to the Cisco AR	12
Description	12
Reference	12
Procedure	12
Notes	12
Configuring, Modifying, and Managing Syslog Messages	13
Description	13

- Reference 13
- Procedure 13
- Setting Up and Managing Accounting 14**
 - Description 14
 - Reference 14
 - Procedure 14
- Modifying Configurations Using aregcmd Commands 15**
 - Description 15
 - Reference 15
 - Procedure 15
- Managing the Cisco AR Using aregcmd Commands 16**
 - Description 16
 - Reference 16
 - Procedure 16
- Backing Up the Database 17**
 - Description 17
 - Reference 17
 - Procedure 17
- Monitoring the UG 18**
 - Description 18
 - Reference 18
 - Procedure 18

CHAPTER 8

Using Cisco IOS for Operations and Maintenance 1

- Introduction 1
 - Target Platforms 1
 - References 1
 - Task Summary 2
 - Monitoring Network Performance 2
 - Managing Gateways 2
 - Managing Gatekeepers 2
 - Managing Modems 2
 - Using MIB Objects 2
- Monitoring Network Performance Using IOS Commands 3
- Managing Gateways 3
 - Checking Memory and CPU Utilization 3
 - Configuring Call Admission Control Thresholds Using Cisco IOS Commands 4
 - Verifying Call Admission Control Configurations 4
 - Verifying Controllers 5

Verifying ISDN PRI	5
Verifying ISDN D-Channels	6
Verifying Universal Port Card and Lines	6
Verifying Clocking	6
Testing Asynchronous Shell Connections	6
Configuring and Verifying Alarms	7
Managing and Viewing SPE Performance Statistics	7
Managing Ports	7
Managing and Troubleshooting SPEs	8
Using Cisco Call Tracker to Manage Gateways	8
Configuring Call Tracker	9
Verifying Call Tracker	9
Managing Gatekeepers	9
Configuring Load Balancing and Alternate Gatekeepers	9
Configuring Remote Clusters	9
Configuring Server Triggers	9
Verifying Gatekeeper Configuration	10
Maintaining and Monitoring Gatekeeper Endpoints	10
Managing Modems	10
Using and Managing MIBs	10
Obtaining MIBs	11
Using MIB Locator	11
Using MIB Objects	12
Cisco IOS References	12
Cisco IOS	12
System Error Messages	13
Debug Command Reference	13

CHAPTER 9

Managing Billing and Accounting Data	1
Introduction	1
Target Platforms	1
References	1
Generating VoIP CDRs	2
Enabling Timestamps	2
With a Network Time Server	2
Without a Network Timeserver	2
A Sample CDR Configuration	2
Collecting Billing and Accounting Data Using Cisco BAMS	3
Setting up Billing Logic	3

Using Operational Measurements 4
 References 4
 Collecting Accounting Data Using Cisco AR 5
 Collecting Accounting Data Using Cisco RPMS 5

CHAPTER 10

Upgrade Considerations 1
 Introduction 1
 Target Platforms 1
 Upgrading All Gateways and Gatekeepers 2
 Upgrading at the Billing Component Level 2
 Upgrading at the Network Management Level 2
 Upgrading the Cisco ASAP Solution 3
 Upgrading Cisco SS7 Interconnect for Voice Gateways Solution 3
 Upgrading the Cisco PSTN Gateway Solution 3

CHAPTER 11

Operating and Maintaining SS7 Components 1
 Introduction 1
 Target Platforms 1
 References 1
 Cisco MGC Release 7 1
 Cisco MGC Release 9 2
 Operations and Maintenance Tasks 2

CHAPTER 12

Provisioning a Cisco MGC Node Using Cisco VSPT 1
 Introduction 1
 Target Platforms 1
 References 2
 Using Cisco VSPT 2
 Release 1.6 2
 Release 2.2 2
 Using MML 2

CHAPTER 13

Troubleshooting SS7 Interconnect Problems: Cisco MGC Node 1
 Introduction 1
 Target Platforms 1
 References 2
 Cisco MGC Release 7 2

Cisco MGC Release 9	2
Task Summary	2
Using System Output	2
Resolving SS7 Network Problems	3
Resolving Bearer Channel Connection Problems	3
Tracing	3
Troubleshooting the Cisco MGC Platform	3
Retrieving All Active Alarms	5
Description	5
Reference	5
Procedure	5
Viewing System Logs	6
Description	6
Reference	6
Procedure	6
Using Alarm Troubleshooting Procedures	7
Description	7
Reference	7
Procedure	7
Notes	7
Restoring an SS7 Link to Service	8
Description	8
Reference	8
Procedure	8
Resolving an SS7 Load Sharing Malfunction	9
Description	9
Reference	9
Procedure	9
Resolving Physical Layer Failures	10
Description	10
Reference	10
Procedure	10
Correcting Bouncing SS7 Links	11
Description	11
Reference	11
Procedure	11
Restoring an SS7 DPC to Service	12
Description	12
Reference	12

Procedure	12
Restoring an SS7 Route to Service	13
Description	13
Reference	13
Procedure	13
Restoring an Unavailable SS7 DPC	14
Description	14
Reference	14
Procedure	14
Notes	14
Verifying MTP Timer Settings	15
Description	15
Reference	15
Procedure	15
Notes	15
Modifying MTP Timer Settings	16
Description	16
Reference	16
Procedure	16
Notes	16
Verifying the Proper Loading of a Dial Plan	17
Description	17
Reference	17
Procedure	17
Notes	17
Querying Local and Remote CIC States	18
Description	18
Reference	18
Procedure	18
Notes	18
Resolving Local and Remote CIC State Mismatch	19
Description	19
Reference	19
Procedure	19
Notes	19
Performing CIC Validation Tests	20
Description	20
Reference	20
Procedure	20

Resolving ISDN D-Channel Discrepancies	21
Description	21
Reference	21
Procedure	21
Unblocking CICs	22
Description	22
Reference	22
Procedure	22
Notes	22
Resetting CICs	23
Description	23
Reference	23
Procedure	23
Notes	23
Resolving Stuck CICs	24
Description	24
Reference	24
Procedure	24
Running a Manual Continuity Test	25
Description	25
Reference	25
Procedure	25
Notes	25
Verifying Continuity Test Settings	26
Description	26
Reference	26
Procedure	26
Notes	26
Restoring a Media Gateway IP Destination/Link to Service	27
Description	27
Reference	27
Procedure	27
Calls Fail at the Cisco MGC	28
Description	28
Reference	28
Procedure	28
Modifying Redundant Link Manager Timers	29
Description	29
Reference	29

Procedure	29
Notes	29
Performing a Call Trace	30
Description	30
Reference	30
Procedure	30
Notes	30
Alternatives to Call Tracing	31
Description	31
Reference	31
Procedure	31
Notes	31
Performing a TCAP Trace	32
Description	32
Reference	32
Procedure	32
Deleting Unnecessary Files	33
Description	33
Reference	33
Procedure	33
Recovering from a Switchover Failure	34
Description	34
Reference	34
Procedure	34
Recovering from Cisco MGC Host(s) Failure	35
Description	35
Reference	35
Procedure	35
Restoring Stored Configuration Data	36
Description	36
Reference	36
Procedure	36
Notes	36
Verifying Proper Configuration of Replication	37
Description	37
Reference	37
Procedure	37
Measurements Are Not Being Generated	38
Description	38

Reference	38
Procedure	38
Call Detail Records Are Not Being Generated	39
Description	39
Reference	39
Procedure	39
Rebooting Your System to Modify Properties	40
Description	40
Reference	40
Procedure	40
Resolving a Failed Connection to a Peer	41
Description	41
Reference	41
Procedure	41

CHAPTER 14**Troubleshooting the Cisco Access Registrar 1**

Introduction	1
Troubleshooting Procedures	1
Useful IOS Commands	1
References	1
RADIUS Server Not Defined	3
Description	3
Reference	3
Procedure	3
Notes	4
RADIUS Keys Mismatched	5
Description	5
Reference	5
Procedure	6
Notes	6
Authorization Incorrectly Configured	7
Description	7
Reference	8
Procedure	8
Notes	8
Using show Commands	9
Description	9
Reference	9
Command	9

Notes 9

Using debug Commands 10

 Description 10

 Reference 10

 Commands 10

 Notes 10

CHAPTER 15

Troubleshooting Using the Cisco Universal Gateway Manager 1

Introduction 1

 References 2

Setting Controller Logging Levels 3

 Description 3

 Reference 3

 Procedure 3

Managing Log Files 4

 Description 4

 Reference 4

 Procedure 4

Troubleshooting Discovery and Deployment 5

 Description 5

 Reference 5

 Procedure 5

Troubleshooting Configuration and Image Management 6

 Description 6

 Reference 6

 Procedure 6

Troubleshooting Fault Management 7

 Description 7

 Reference 7

 Procedure 7

Troubleshooting Performance Management 8

 Description 8

 Reference 8

 Procedure 8

Troubleshooting the Configure Administrative State Function 9

 Description 9

 Reference 9

 Procedure 9

Troubleshooting IOS Operations	10
Description	10
Reference	10
Procedure	10
CHAPTER 16	Troubleshooting the Cisco RPMS 1
Introduction	1
System Installation and Startup	1
GUI Access	2
Operational Problems	2
Related IOS Commands	2
References	2
Archive Extraction Error	3
Description	3
Reference	3
Procedure	4
Database Initialization Failure	5
Description	5
Reference	5
Procedure	5
Database Connectivity Failure	7
Description	7
Reference	7
Procedure	7
Notes	8
Web Server Fails to Start	9
Description	9
Reference	9
Procedure	9
Unable to Start/Stop Oracle	10
Description	10
Reference	10
Procedure	10
Unable to Start/Stop TNS Listener	12
Description	12
Reference	12
Procedure	12
Images on the Cisco RPMS GUI Are Not Displayed Correctly	14
Description	14

Reference	14
Procedure	14
Unable to Add/Change/Delete Administrators in the GUI	15
Description	15
Reference	15
Procedure	15
RPMS Server Process Is Not Running	16
Description	16
Reference	16
Procedure	16
Notes	16
RPMS Database Server Process Is Not Running	17
Description	17
Reference	17
Procedure	17
Notes	18
RPMS Watchdog Process Is Not Running	19
Description	19
Reference	19
Procedure	19
Incorrect Access Server and Cisco RPMS Keys	20
Description	20
Reference	20
Procedure	20
Notes	20
Cisco RPMS Cannot Identify Access Server	21
Description	21
Reference	21
Procedure	21
Notes	22
TACACS+ Single Connection Is Configured	23
Description	23
Reference	23
Procedure	23
Port Counts Are Out of Synchronization	24
Description	24
Reference	24
Procedure	24
Oracle Configuration Updates Are Not Reflected on Snapshot Site Cisco RPMS Server(s)	25

Description	25
Reference	25
Procedure	25
Enabling a Cisco RPMS Debugging Session	27
Description	27
Reference	27
Procedure	27
Disabling a Cisco RPMS Debugging Session	28
Description	28
Reference	28
Procedure	28
Using show Commands	29
Description	29
Reference	29
Commands	29
Using debug Commands	30
Description	30
Reference	30
Commands	30
CHAPTER 17	Maintaining and Troubleshooting Cisco WAN Switches 17-1
Introduction	17-1
Target Platforms	17-1
References	17-1
Using the Voice Interworking Service Module, Release 3.0	17-2
Configuring VISM Features	17-2
VISM CLI Commands	17-2
Troubleshooting VISM	17-2
Maintaining the MGX Route Processor Module	17-3
Recovering a Lost Password	17-3
Using Cisco MGM, Release 2.0	17-3
Cisco MGM User Interfaces	17-3
Cisco MGM Configuration	17-3
Cisco MGM Administration	17-4
Cisco MGM Fault and Performance Management	17-4
Cisco MGM Security	17-4
Using Cisco WAN Manager, Release 10.5	17-4

GLOSSARY

INDEX



Preface

This operations, maintenance, and troubleshooting guide is designed to be used with the following solutions:

- Cisco ASAP Solution
- Cisco PSTN Gateway Solution
- Cisco SS7 Interconnect for Voice Gateways Solution



Note

This document refers to the Cisco PSTN Gateway Solution and the Cisco SS7 Interconnect for Voice Gateways Solution as PSTN gateway solutions.

This document addresses issues related to the resources, components, and traffic of such networks. Cisco applications that use a graphical user interface (GUI) for ease of use are presented first. However, many capabilities are available through the command-line interface (CLI) of the Cisco IOS, as well as the MML (man machine language) software that is used to manage the Cisco SC2200 or Cisco PGW 2200 host. A variety of application documents also provide CLI alternatives to functions.



Note

The Cisco PGW 2200 configured for signaling is also referred to in a variety of documents as the Cisco SC2200, the earlier term. The term “Cisco SC2200” is applicable to the Cisco ASAP Solution and Release 1.3 of the Cisco SS7 Interconnect for Voice Gateways Solution, and the term “Cisco PGW 2200” is applicable to the Cisco PSTN Gateway Solution and Release 2.0 of the Cisco SS7 Interconnect for Voice Gateways Solution.

It is not expected that you have all the applications, or that you need to manage all the components, that are discussed here. Nevertheless, this guide can also serve as a resource for understanding the various features of each application. In some cases a variety of applications can be used to achieve the same objective.

Finally, this guide is meant to provide a high-level view only, and does not attempt to cover all the features and details of the applications discussed here. Always rely on the standard documentation for those applications for the details of installing, using, and troubleshooting. Links to the latest documentation are provided in the appropriate chapters of this guide. While this document has tried to be as current as possible, the documentation for applications is subject to revision. Information is subject to reorganization, section headings are subject to renaming, and hyperlinks are subject to change. Nevertheless, many of the general principals and practices referred to from the *Cisco Integrated Network Solutions Operations, Maintenance, and Troubleshooting Guide* can continue to be of value until this document is revised.

The most recent versions of this guide and related documentation can be found at the following URL:

<http://www.cisco.com/univercd/cc/td/doc/product/access/sc/re19/soln/voip20/index.htm>

**Note**

All Cisco solutions documents can be found under Cisco Solutions, at the following URL:
<http://www.cisco.com/univercd/cc/td/doc/solution/index.htm>

This preface presents the following major topics:

- [Document and Solution Release](#)
- [Audience](#)
- [Scope](#)
- [Document Organization](#)
- [Related Documents](#)
- [Document Conventions](#)
- [Obtaining Documentation](#)
- [Obtaining Technical Assistance](#)

Document and Solution Release

This release of this document covers Release 1.0 of the Cisco ASAP Solution, the Cisco PSTN Gateway Solution, Releases 1.3 and 2.0 of the Cisco SS7 Interconnect for Voice Gateways Solution. Those solutions are referred to generically in this document, that is, without their release numbers.

Future updates to this document will be indicated in the following table.

Document Version Number	Date	Notes
1	04/17/02	This document was first released to limited distribution.
2	05/14/02	Distinctions were noted between releases of the Cisco SS7 Interconnect for Voice Gateways Solution, along with related use of the terms “Cisco SC2200” and “Cisco PGW 2200.”
3	07/25/02	Cisco PSTN Gateway Solution platforms were added.

Audience

The target audience for this document is assumed to have basic knowledge in the following areas:

- Familiarity with basic UNIX commands and operations, in order to configure the Cisco SC2200 or Cisco PGW 2200
- Familiarity with configuring T1/E1 CAS and PRI signaling on the Cisco AS5000 series
- Familiarity with configuring a basic H.323 gateway on the Cisco AS5000 series
- Familiarity with configuring a basic H.323 gatekeeper on the Cisco 3600 or 7200 series
- Familiarity with the Cisco Wholesale Voice Solution

**Note**

For documentation on all Cisco solutions, refer to Cisco Solutions at the following URL:
<http://www.cisco.com/univercd/cc/td/doc/solution/index.htm>

Scope

This document presents the fundamental operations, maintenance, and troubleshooting information that is required for the various services provided by the Cisco ASAP Solution and the Cisco SS7 Interconnect for Voice Gateways Solution. Service provider networks may have additional requirements that are beyond the scope of this document. In addition, this document is primarily for Cisco products. To establish and maintain third-party products and applications that may be a part of these solutions, refer to the documentation provided by the vendors of those products.

Most chapters in this document apply to all Cisco Integrated Network Solutions. The chapters that do not apply to all three solutions are listed below:

Section	Title	Solutions
Chapter 2	Managing Network Elements and Dial Plans: Using Cisco Voice Manager	Cisco ASAP Solution Cisco SS7 Interconnect Solution
Chapter 3	Managing Resources and Dial Services: Using Cisco RPMS	Cisco ASAP Solution Cisco PSTN Gateway Solution
Chapter 4	Managing Network Objects: Using Cisco UGM	Cisco ASAP Solution Cisco PSTN Gateway Solution
Chapter 6	Operating and Maintaining Cisco Devices: Using Cisco Info Center	Cisco ASAP Solution only.
Chapter 7	Operating and Maintaining the Cisco Access Registrar	Cisco ASAP Solution only.
Chapter 14	Troubleshooting the Cisco Access Registrar	Cisco ASAP Solution only.
Chapter 15	Troubleshooting Using the Cisco Universal Gateway Manager	Cisco ASAP Solution Cisco PSTN Gateway Solution
Chapter 16	Troubleshooting the Cisco RPMS	Cisco ASAP Solution Cisco PSTN Gateway Solution
Chapter 17	Maintaining and Troubleshooting Cisco WAN Switches	Cisco PSTN Gateway Solution only.

Document Organization

The major sections of this document are as follows:

Section	Title	Major Topics
Chapter 1	How to Use This Guide	Introduces the various tools, their place in the network, and the services they provide. Maps operations and management (O&M) topics to the tools. Introduces basic O&M guidelines.
Chapter 2	Managing Network Elements and Dial Plans: Using Cisco Voice Manager	Presents O&M tasks available through CiscoWorks2000 Voice Manager. Tasks include managing network elements, dial plans, and voice ports.
Chapter 3	Managing Resources and Dial Services: Using Cisco RPMS	Presents O&M tasks available through Cisco RPMS. Tasks include configuring call discrimination, configuring resource management, configuring dial services, viewing server reports, and administering the server.
Chapter 4	Managing Network Objects: Using Cisco UGM	Presents O&M tasks available through Cisco Universal Gateway Manager. Tasks include deploying, discovering, and exporting inventory data; configuring devices, managing images and scheduling actions; configuring the administrative state of objects; managing security; managing device performance; and managing faults.
Chapter 5	Managing SS7 Signaling Components: Using Cisco MGC Node Manager	Presents O&M tasks available through Cisco Media Gateway Controller Node Manager. Tasks include managing security; deploying a site, object, or network; using polling to monitor network performance; managing traps and events; and viewing information about network devices.
Chapter 6	Operating and Maintaining Cisco Devices: Using Cisco Info Center	Presents O&M tasks available through Cisco Info Center. Tasks include starting and stopping the Cisco Info Server; creating a new server; displaying alerts; managing the server; managing objects; and creating, editing, and managing views.
Chapter 7	Operating and Maintaining the Cisco Access Registrar	Presents O&M tasks available through the Cisco Access Registrar CLI. Tasks include configuring clients, profiles, groups, multiple user lists, remote servers, and session management; validating new configurations; checking the AR server; configuring, modifying, and managing syslog messages; setting up and managing accounting; modifying configurations and managing the Cisco AR using aregcmd commands; backing up the database; and monitoring the UG.

Chapter 8	Using Cisco IOS for Operations and Maintenance	Presents a variety of Cisco IOS commands that can be used directly on UGs and GKs to perform tasks such as the following (among others): managing memory and CPU use; verifying controllers; verifying universal port cards and lines; configuring and verifying alarms; managing ports and SPEs; managing GKs; managing modems; managing Cisco SC2200 and Cisco PGW 2200 nodes; and using MIB objects.
Chapter 9	Managing Billing and Accounting Data	Discusses general considerations that customers need to make when upgrading a Cisco Integrated Network Solution.
Chapter 10	Upgrade Considerations	Discusses general considerations that customers need to make when upgrading the Cisco ASAP Solution or the Cisco SS7 Interconnect for Voice Gateways Solution.
Chapter 11	Operating and Maintaining SS7 Components	Presents references to a variety of operations and maintenance practices specific to networks that support SS7 interconnect.
Chapter 12	Provisioning a Cisco MGC Node Using Cisco VSPT	Provides references for how to use the Cisco Voice Services Provisioning Tool (VSPT) to provision Cisco Media Gateway Controller (MGC) nodes, such as a Cisco SC2200 Signaling Controller to support SS7 signaling. Cisco VSPT provides for the creation, modification, and execution of signaling connections, trunk groups, trunks, routes, and dial plans.
Chapter 13	Troubleshooting SS7 Interconnect Problems: Cisco MGC Node	Presents a variety of troubleshooting methods not presented in previous chapters. Covers tasks performed from the following tools: Cisco Info Center, Cisco UGM, CMNM, and SS7 interconnect components.
Chapter 14	Troubleshooting the Cisco Access Registrar	Presents troubleshooting tasks for the Cisco Access Registrar (AR) as they relate to the Cisco ASAP Solution.
Chapter 15	Troubleshooting Using the Cisco Universal Gateway Manager	Presents troubleshooting tasks related to the Cisco ASAP Solution and the Cisco PSTN Gateway Solution that are provided from the Cisco Universal Gateway Manager (Cisco UGM).
Chapter 16	Troubleshooting the Cisco RPMS	Presents operations and maintenance tasks related to the Cisco ASAP Solution that are provided from Cisco RPMS.
Chapter 17	Maintaining and Troubleshooting Cisco WAN Switches	Presents operations, maintenance, and troubleshooting tasks for the MGX/VISM as they relate to Cisco PSTN Gateway Solution.

Glossary	Glossary	Defines abbreviated terms used in this and related documents.
Index	Index	

Related Documents

The majority of the documents referred to in the *Cisco Integrated Network Solutions Operations, Maintenance, and Troubleshooting Guide* are available online. They are discussed as you need to refer to them. In the electronic (PDF) version of this document you can click on the URL (Uniform Resource Locator, often referred to as the website) associated with the title of a document, and the selected document will appear within the Adobe Acrobat application window. You can also use the Text Select Tool (third icon from the top, at the left of the Acrobat application window) to copy a URL from the PDF document and paste it into the location field of your browser.

Viewing Online Documents in Your Browser

As you click on links, the files you select may be added to the current document. When you close the file, you will be prompted to save the file. (You will not be able to save the file to a CD.) If you choose not to save the larger file that is created, click *No* when prompted to save the file. However, if you acquire documents that you want to save in a new file, you can save that file to another disk or drive with a new name of your own choosing. Set the following preferences within the Acrobat application to open weblinks in your browser, rather than within Acrobat.

You can obtain the latest version of Adobe Acrobat Reader at <http://www.adobe.com>.

-
- Step 1** Select the browser you want to use.
- a. From the Acrobat main menu, choose File > Preferences > Weblink. The Weblink Preferences window opens.
 - b. In the Weblink Preferences window, click Browse (or Select) and locate the browser you wish to use.
 - c. Then select Connection Type from the pull-down menu. Choose Standard if your browser is not listed.
 - d. Click OK to save your settings.
- Step 2** Make sure that Acrobat opens weblinks in your browser.
- a. From the Acrobat main menu, choose File > Preferences > Web Capture. The Web Capture Preferences window opens.
 - b. In the Web Capture Preferences Window, choose Open Weblinks: In Web Browser.
 - c. Click OK to save your settings.
-

Document Conventions

Command descriptions use the following conventions:

boldface font	Commands and keywords are in boldface .
<i>italic font</i>	Arguments for which you supply values are in <i>italics</i> .
[]	Elements in square brackets are optional.
{ x y z }	Alternate keywords are grouped in braces and separated by vertical bars.

[x y z]	Optional alternative keywords are grouped in brackets and separated by vertical bars.
string	A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.

Screen examples use the following conventions:

screen font	Terminal sessions and information the system displays are in <i>screen font</i> .
boldface screen font	Information you must enter is in boldface screen font . ¹
<i>italic screen font</i>	Arguments for which you supply values are in <i>italic screen font</i> .
→	This pointer highlights an important line of text in an example.
^	The symbol ^ represents the key labeled Control. For example, the key combination ^D in a screen display means hold down the Control key while you press the D key.
< >	Nonprinting characters, such as passwords, are in angle brackets in contexts where italic font is not available. Also used to represent variables in command line examples where <i>screen font</i> is used.
[]	Default responses to system prompts are in square brackets.
!, #	An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.

1. As this document makes use of annotated configurations, the rigorous use of boldface type to indicate what the user must enter is relaxed.

Notes use the following conventions:



Note

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

Timesavers use the following conventions:



Timesaver

This symbol means *the described action saves time*. You can save time by performing the action described in the paragraph.

Cautions use the following conventions:



Caution

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

Tips use the following conventions:

**Tip**

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

Obtaining Documentation

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

World Wide Web

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

<http://www.cisco.com>

To view this site in another language, click **Countries/Languages** at the top of the page.

Documentation CD-ROM

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

Ordering Documentation

Cisco documentation is available in the following ways:

- Registered Cisco Direct Customers can order Cisco Product documentation from the Networking Products MarketPlace:
http://www.cisco.com/cgi-bin/order/order_root.pl
- Registered Cisco.com users can order the Documentation CD-ROM through the online Subscription Store:
<http://www.cisco.com/go/subscription>
- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco corporate headquarters (California, USA) at 408 526-7208 or, in North America, by calling 800 553-NETS(6387).

Documentation Feedback

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

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

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

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

We appreciate your comments.

Obtaining Technical Assistance

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

Cisco.com

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

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

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

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

<http://www.cisco.com>

Technical Assistance Center

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

Contacting TAC by Using the Cisco TAC Website

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

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

P3 and P4 level problems are defined as follows:

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

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

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

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

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

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

Contacting TAC by Telephone

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

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

P1 and P2 level problems are defined as follows:

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



How to Use This Guide

Overview

This chapter provides an overview of the contents of this guide. Although the focus is on the general tasks required to manage and maintain the Cisco ASAP Solution and the PSTN gateway solutions, much of what is available here is useful in a variety of other situations.



Note

PSTN gateway solutions include Cisco PSTN Gateway Solution and Cisco SS7 Interconnect for Voice Gateways Solution.

The means to achieve these tasks include not only Cisco proprietary element and network management tools with graphical user interfaces (GUIs), but also commands that can be issued from the command line interface (CLI).

This document addresses only those activities following the initial “first day” installation that are required to enable features, add or delete subscribers and resources, or conduct other ongoing activities—either as-needed or scheduled—that must be done to maintain network services. It is assumed that all of the components of this solution have been correctly installed, configured, and provisioned, and that a basic solution network has been brought into service. (See [Prerequisites](#), below.)

For an overview of the topics in each chapter, refer to [Document Organization](#), page xxxii.

This chapter covers the following major topics:

- [Operations and Maintenance Tasks: At a Glance](#)
- [Resource and Network Performance Management](#)
- [Troubleshooting and Trouble Clearing Tasks: At a Glance](#)



Note

This guide is meant to provide a high-level view only, and does not attempt to cover all the features and details of the applications discussed here. Always rely on the standard documentation for those applications for the details of installing, using, and troubleshooting. Links to the latest documentation are provided in the appropriate chapters of this guide. While this document has tried to be as current as possible, the documentation for applications is subject to revision. Information is subject to reorganization, section headings are subject to renaming, and hyperlinks are subject to change.

Prerequisites

The information herein is useful in a variety of situations, but an attempt has been made to focus on the needs of the following solutions:

- Cisco ASAP Solution
- PSTN gateway solutions
 - Cisco PSTN Gateway Solution
 - Cisco SS7 Interconnect for Voice Gateways Solution

References for those solutions are provided below. Before proceeding, take the time to familiarize yourself with the requirements and applications of those solutions.

Cisco ASAP Solution References

In order to operate and maintain the Cisco ASAP Solution, make sure you have read the following documents:

- *Cisco ASAP Solution Overview and Planning Guide*
- *Cisco ASAP Solution Implementation Guide*
- *Cisco ASAP Solution 1.0 Release Notes*

These are available at the Cisco Any Service, Any Port Solution web site, at the following URL:

<http://www.cisco.com/univercd/cc/td/doc/product/access/solution/asap/index.htm>

For an overview of solution-related network management tools and their function in the Cisco ASAP Solution, refer to the “Chapter 5, Solution Management” of the *Cisco ASAP Solution Overview and Planning Guide*. In addition to these tools, you can use the Cisco IOS CLI commands to install, configure, operate, monitor, and troubleshoot the Cisco ASAP Solution components.

PSTN Gateway Solutions References

Cisco SS7 Interconnect for Voice Gateways Solution References

In order to operate and maintain the Cisco SS7 Interconnect for Voice Gateways Solution, make sure you have read the following documents:

- *Cisco SS7 Interconnect for Voice Gateways Solution Master Index*
- *Cisco SS7 Interconnect for Voice Gateways Solution Overview and Planning Guide*
- *Cisco SS7 Interconnect for Voice Gateways Solution Implementation Guide*
- *Cisco SS7 Interconnect for Voice Gateways Solution Release Notes*
- *Cisco SS7 Interconnect for Voice Gateways Solution Upgrade Guide* (if upgrading from a previous version of this solution)

These are available at the Cisco SS7 Interconnect for Voice Gateways Solution web site, at the following URLs:

<http://www.cisco.com/univercd/cc/td/doc/product/access/sc/re19/soln/voip20/index.htm>

Cisco PSTN Gateway Solution References

In order to operate and maintain the Cisco PSTN Gateway Solution, make sure you have read the following documents:

- *Cisco PSTN Gateway Solution Solution Master Index*
- *Cisco PSTN Gateway Solution Solution Release Notes*
- *Cisco PSTN Gateway Solution Platform Documentation*
- *Cisco PSTN Gateway Solution Application Notes*

These are available at the Cisco PSTN Gateway Solution web site, at the following URLs:

<http://www.cisco.com/univercd/cc/td/doc/solution/dialvoic/pstngw/index.htm>

Operations and Maintenance Tasks: At a Glance

There are a variety of tasks that Cisco recommends you attend to on a rigorously scheduled basis. Other tasks can simply be done as needed, although you may want to schedule certain critical tasks depending on the needs of your network. This section presents the following topics:

- [Regularly Scheduled Tasks](#)
- [General Operations and Maintenance Guidelines](#)
- [As-Needed Tasks](#)

Regularly Scheduled Tasks

Table 1-1 identifies, at a high level, the tasks that service providers must do on a daily, weekly, monthly, and annually basis to operate and maintain the health of their Cisco ASAP Solution or PSTN gateway solutions network.

Table 1-1 Regularly Scheduled Operations and Maintenance Tasks

Frequency	Task	Notes
Daily	Monitor alarms from all platforms in network	View alarms on platform directly, or use a network management system.
	Review system logs	This is especially important on the Cisco SC2200 or Cisco PGW 2200 host.
	Monitor availability of disk space on Cisco SC2200 host	
	Monitor peak call rates on Cisco SC2200 host	
	Monitor CDRs and other billing records for accuracy, and age-flag records for deletion and archiving	The service provider will need to develop a process for determining when records can be removed from the host and archived.

Table 1-1 Regularly Scheduled Operations and Maintenance Tasks

Frequency	Task	Notes
Weekly	Back up all relevant data and configuration information for all network platforms.	The service provider will need to develop a process for determining what “relevant” means and what platforms are at issue.
	Visit Cisco websites regularly to see whether Solution release notes have been updated to recommend new software releases.	As new releases become available and caveats are added or resolved, the solution release notes will be updated to keep information as current as possible.
Monthly	In a maintenance window, test the ability of Cisco SC2200 node components to failover from active to standby.	If failover is not tested regularly, redundant equipment is of little value.
Annually	Plan for the possibility of a major network upgrade of Cisco software.	This includes Cisco IOS and software for the Cisco SC2200 or Cisco PGW 2200 host. Changes may be required in hardware, particularly in memory.
	Review overall network traffic requirements to ensure that traffic is being served properly by existing network.	

General Operations and Maintenance Guidelines

To maintain your solution network, follow these general best practices for your solution network:

- Develop a general strategy for monitoring the Cisco PGW2200, Cisco AS5000 series access servers, Cisco RPMS, and the Cisco Access Registrar servers.
- Develop a general strategy for monitoring the Cisco MGX8000 series and Cisco Voice Interworking Service Module (VISM).
- Use the software tools available on each platform to monitor and report critical data such as modem health, SPE health, T1/E1/T3 facility health, IP network integrity, SS7 network performance and stability, SS7 call processing success, voice and modem call success, voice quality, and fault alarms.
- Check equipment status.
- Regularly monitor system log entries.
- Regularly issue status queries, using either a variety of GUI element-management tools, or Cisco IOS (see [Chapter 8, “Using Cisco IOS for Operations and Maintenance”](#)) or MML (Man Machine Language) commands entered at the CLI.
- When removing or add any of the solution components, be sure to read thoroughly the most recent applicable hardware and software documents.
- Be sure that you provide for redundancy before upgrading any of the solution components.

[Table 1-2](#) lists general operations and maintenance guidelines (parameters to monitor) for a variety of Cisco applications, platforms, and network types. (Cisco AS5000 series access servers include both universal gateways and dial-only/voice-only gateways.)

Table 1-2 General Operations and Maintenance Guidelines

Subject	Parameters to Monitor	Notes
Cisco Access Registrar	CPU load and memory use	
	Rejected requests	See Chapter 7, “Operating and Maintaining the Cisco Access Registrar.”
	Timeouts	
	Call completions	
	Accounting records	
Cisco RPMS	CPU load and memory use	
	Cisco RPMS reports	See Chapter 3, “Managing Resources and Dial Services: Using Cisco RPMS.”
	Accounting records	
Cisco SC2200 or PGW 2200 Node	Availability of Cisco SC2200 or PGW 2200 host	Use rtrv-ne (see first Note below).
	Status of SS7 from PSTN	For Release 7 of the Cisco MGC software, use rtrv-sc:all to retrieve the status of SS7 from PSTN. For Release 9 of the Cisco MGC software, use rtrv-c7lnk:all to retrieve the status of SS7 from PSTN.
	Daemons on Cisco SC2200 host	Use rtrv-softw:all , to check for proper operation.
	Ethernet interface connecting Cisco SC2200 host to Cisco SLT	Use ifconfig -a .
	CPU load and memory use	For Release 7 of the Cisco MGC software, use ps -ef -o user,pid,pcpu -o args to retrieve CPU load data and vmstat to retrieve virtual memory data. For Release 9 of the Cisco MGC software, use rtrv-ne-health::all to retrieve CPU load and virtual memory data.
	Alarms	Use rtrv-alm::cont to retrieve alarms on a continuous basis.
	Measurements related to SS7 and PRI status	These and other similar measurements are available in Cisco SC2200 Release 7.4(12).
	Call completion rates	Use rtrv-ctr .
	Call performance statistics: <ul style="list-style-type: none"> • number of active calls • number of redirected calls • number of rejected calls • number of busy calls 	Use rtrv-ctr .
	System logs and network outages in network backbone	Applies to Cisco SC (MGC) node components: Cisco SLT, Cisco BAMS, Cisco SC2200 host. See second Note below.
	On the SLT: status of interface (up/down ~ active/inactive)	
On the SLT: CPU load and memory use		

Table 1-2 General Operations and Maintenance Guidelines (continued)

Subject	Parameters to Monitor	Notes
Cisco AS5000 Series Access Servers	CPU load and memory use	
	Modem call completion	
	Connection rates and speeds	
	Voice call completion	
	Health of controllers (T1/E1/T3)	
	If Call Admission Control (CAC) is configured, call threshold status	
	If Cisco AR is configured, the RADIUS statistics for the gateway	
	Continuity test (COT) statistics	
Cisco Gatekeeper	CPU load and memory use	
Cisco VISM	Card LED	
	Logs	
	Display	
	Alarms	
VoIP Networks	CPU load and memory use on gateways	
	Packet loss	
	Packet jitter	
	Delay	

**Note**

For syntax descriptions of these and other MML commands, refer to Chapter 2, “MML Commands,” of the *Cisco Media Gateway Controller Software MML Command Guide* appropriate to the release of the Cisco MGC software running on your system. The documents for the releases are available at the following URLs:

Release 7:

<http://www.cisco.com/univercd/cc/td/doc/product/access/sc/re17/r7mmlref/index.htm>

Release 9:

<http://www.cisco.com/univercd/cc/td/doc/product/access/sc/re19/mmlref/mmlow.htm>

**Note**

For information about managing the MGC node, including daily tasks, periodic maintenance, and regular operations procedures, refer to Chapter 3, “Operating Procedures” of the *Cisco MGC Software Release 7 Operations, Maintenance, and Troubleshooting Guide* or the *Cisco MGC Software Release 9 Operations, Maintenance, and Troubleshooting Guide*. Release 7 applies to the Cisco ASAP Solution and Release 1.3 of the Cisco SS7 Interconnect for Voice Gateways Solution, and Release 9 applies to Release 2.0 of the Cisco SS7 Interconnect for Voice Gateways Solution and the Cisco PSTN Gateway Solution. See [Chapter 11, “Operating and Maintaining SS7 Components.”](#)

As-Needed Tasks

Table 1-3 lists the operations and maintenance tasks that are generally done as needed (for example, adding new equipment to support new subscribers, or adding a new dial plan to accommodate a new geographical region), although they can also be done in accordance with a schedule depending on the needs of the network. Troubleshooting chapters specific to various applications are also listed. Tasks are sorted first by the components to which they apply. Some tools provide management capabilities but must be managed themselves. In addition, some tasks may be repeated, because they fall into multiple categories.



Tip

Take the time to become familiar with the varieties of tasks and the tools that support them.

Any of these tasks may be performed to establish, change, or discontinue service—either in response to customer demand or to optimize the performance of equipment or software configurations. The following legend lists the acronyms used for the tools in the table.

Because this document covers the breadth of applications for the Cisco Integrated Network Solutions, it is not expected that you have all the applications that are discussed here, or that you need to manage all the components.



Note

The network management applications that can be used to manage the Cisco SS7 Interconnect for Voice Gateways Solution are as follows: Cisco BAMS, CMNM, and Cisco VSPT.



Note

The network management applications that can be used to manage the Cisco PSTN Gateway Solution are as follows: Cisco BAMS, CMGM, CMNM, CUGM, RPMS, and Cisco VSPT.

Legend

BAMS	Cisco Billing and Measurements Server
CAR	Cisco Access Registrar
CIC	Cisco Info Center
CMNM	Cisco Media Gateway Controller Node Manager
CUGM	Cisco Universal Gateway Manager
CVM	Cisco Voice Manager
IOS	Cisco IOS
RPMS	Cisco Resource Pool Manager Server
VSPT	Cisco Voice Services Provisioning Tool

Table 1-3 As-Needed Operations and Maintenance Tasks

Managed Component	Subtopic	Tool	Task
Gateways	Managing Networks	CVM	Creating, Modifying, and Deleting a UG Group, page 2-3
			Adding, Modifying, Locating, and Deleting a UG, page 2-7
			Moving a UG, page 2-9
		CUGM	Deploying and Discovering Network Objects, page 4-3
			Managing and Exporting Inventory Data, page 4-4
			Managing Redundancy and High Availability, page 4-5
			Configuring Managed Devices, page 4-6
			Managing Images and Scheduling Actions, page 4-8
			Configuring the Administrative State of Objects, page 4-9
			Managing Security on Cisco UGM-Managed Devices, page 4-10
			Managing Device Performance, page 4-11
			Managing Faults, page 4-12
			Managing Presence Polling and Loss of Communication, page 4-13
Gateways	Monitoring Network Performance	IOS	Checking Memory and CPU Utilization, page 8-3
			Configuring Call Admission Control Thresholds Using Cisco IOS Commands, page 8-4
			Verifying Call Admission Control Configurations, page 8-4
			Verifying Controllers, page 8-5
			Verifying ISDN PRI, page 8-5
			Verifying ISDN D-Channels, page 8-6
			Verifying Universal Port Card and Lines, page 8-6
			Verifying Clocking, page 8-6
			Testing Asynchronous Shell Connections, page 8-6
			Configuring and Verifying Alarms, page 8-7
			Managing and Viewing SPE Performance Statistics, page 8-7
			Managing and Troubleshooting SPEs, page 8-8
			Using Cisco Call Tracker to Manage Gateways, page 8-8

Table 1-3 As-Needed Operations and Maintenance Tasks (continued)

Managed Component	Subtopic	Tool	Task
Gateways	Managing Subscribers and Ports	CVM	Creating, Modifying, and Deleting a Local Dial Plan, page 2-11
			Creating, Modifying, and Deleting a Network Dial Plan, page 2-12
			Modifying FXO, FXS, E&M, and ISDN Voice Ports, page 2-13
		RPMS	Configuring Port Management: Configuring DNIS Groups, page 3-16
			Configuring Port Management: Configuring Trunk Groups, page 3-18
			Configuring Port Management: Understanding Call Types, page 3-19
		CUGM	Configuring the Administrative State of Objects, page 4-9
	IOS	Managing Ports, page 8-7	
	Managing Modems	IOS	Managing Modems, page 8-10
	Synchronizing GWs and GKs	CVM	Synchronizing Devices, page 2-8
Managing Resources	RPMS	Configuring Port Management: Configuring DNIS Groups, page 3-16	
		Configuring Port Management: Configuring Trunk Groups, page 3-18	

Table 1-3 As-Needed Operations and Maintenance Tasks (continued)

Managed Component	Subtopic	Tool	Task
Gateways	Managing Faults, Alarms, and Traps	CUGM	Managing Faults, page 4-12
		CIC	Using the Event List to Display Alerts, page 6-9
			Managing Objects Using the Objective View, page 6-13
			Creating, Editing, and Managing Filters Using the Filter Builder, page 6-15
		Creating, Editing, and Managing Views Using View Builder, page 6-16	
	Managing Reports and Data	CUGM	Managing Device Performance, page 4-11
	Task Management	CVM	Scheduling Tasks, page 2-10
	Managing Data and Reports	CUGM	Managing and Exporting Inventory Data, page 4-4
	Using CIC to Manage GWs	CIC	Manually Starting and Stopping CIC Components, page 6-4
			Starting and Stopping the Cisco Info Server, page 6-5
			Modifying Configurations Using the Configuration Manager, page 6-6
			Configuring Remote Processes Using Process Control, page 6-7
			Creating a New Cisco Info Server, page 6-8
			Using the Event List to Display Alerts, page 6-9
			Managing the Cisco Info Server Using CLI Options, page 6-10
			Creating and Editing the Interfaces File, page 6-12
			Managing Objects Using the Objective View, page 6-13
			Managing User Access, page 6-14
		Creating, Editing, and Managing Filters Using the Filter Builder, page 6-15	
		Creating, Editing, and Managing Views Using View Builder, page 6-16	
Using Cisco AR to Configure RADIUS Proxy Support	CAR	Configuring Clients, page 7-4	
		See also <i>Managed Components > Cisco AR</i> in this table.	
		Configuring Profiles, page 7-5	
		Validating Configurations, page 7-6	
		Configuring Groups, page 7-7	
	Configuring Multiple UserLists, page 7-8		
Troubleshooting	CIC	Troubleshooting: Using CIC Diagnostic Tools, page 6-17	
	CUGM	Chapter 15, “Troubleshooting Using the Cisco Universal Gateway Manager”	

Table 1-3 As-Needed Operations and Maintenance Tasks (continued)

Managed Component	Subtopic	Tool	Task
Gatekeepers	Managing Networks	CVM	Adding, Modifying, and Deleting a Gatekeeper, page 2-4
			Creating, Modifying, and Deleting a Local Zone on a GK, page 2-5
			Creating, Modifying, and Deleting a Remote Zone on a GK, page 2-6
	Managing Network Performance	IOS	Checking Memory and CPU Utilization, page 8-3
			Configuring Load Balancing and Alternate Gatekeepers, page 8-9
			Configuring Remote Clusters, page 8-9
			Configuring Server Triggers, page 8-9
			Verifying Gatekeeper Configuration, page 8-10
	Maintaining and Monitoring Gatekeeper Endpoints, page 8-10		
	Synchronizing GWs and GKs	CVM	Synchronizing Devices, page 2-8
	Using CIC to Manage GKs	CIC	See Using CIC for Gatekeepers, above.
Troubleshooting	CUGM	Chapter 15, “Troubleshooting Using the Cisco Universal Gateway Manager”	

Table 1-3 As-Needed Operations and Maintenance Tasks (continued)

Managed Component	Subtopic	Tool	Task
SS7 Networks	Managing Networks	CMNM	Configuring Network Devices for Management, page 5-4
			Deployment: Using a Seed File to Deploy a Cisco MGC Network, page 5-6
			Deployment: Manually Deploying a Site, Object, or Network, page 5-7
			Discovery: Discovering a Cisco SLT, LAN Switch, Cisco MGC Host, or BAMS, page 5-9
			Managing Software Images and Configurations, page 5-10
	Managing Reports and Data	CMNM	Monitoring Network Performance: Setting Polling Parameters, page 5-11
			Monitoring Network Performance: Viewing and Managing Performance Data, page 5-13
			Viewing Information about Network Devices: Available Information, page 5-22
			Viewing Information about Network Devices: Using Diagnostic Tools, page 5-24
			Event Messages: BAMS, Cisco MGC, and Cisco MNM, page 5-26
	Managing Faults, Alarms, and Traps	CMNM	Managing Traps and Events: Managing, Clearing, and Forwarding Traps, page 5-15
			Managing Traps and Events: Managing Events, page 5-17
			Managing Traps and Events: Miscellaneous Tasks, page 5-19
			Managing Traps and Events: Setting How Long Alarms are Stored, page 5-21
	Security	CMNM	Setting Up Cisco MNM Security, page 5-5
Troubleshooting	IOS, MML	Chapter 13, “Troubleshooting SS7 Interconnect Problems: Cisco MGC Node”	

Table 1-3 As-Needed Operations and Maintenance Tasks (continued)

Managed Component	Subtopic	Tool	Task
Cisco RPMS	Administration	RPMS	Cisco RPMS Server Administration: Configuring Cisco RPMS Settings, page 3-4
			Cisco RPMS Server Administration: Configuring Administrators and Administrators' Privileges, page 3-5
			Cisco RPMS Server Administration: Configuring Alert Notifications and Logging, page 3-6
			Cisco RPMS Server Administration: Configuring RADIUS Vendors and VSAs, page 3-7
			Cisco RPMS Server Administration: Communicating with Universal Gateways, page 3-9
			Cisco RPMS Server Administration: Configuring AAA Servers, page 3-10
			Cisco RPMS Server Administration: Configuring SNMP Management, page 3-12
			Cisco RPMS Server Administration: Resetting Counters, page 3-13
			Cisco RPMS Server Administration: Managing the Universal Gateway Heartbeat, page 3-14
			Cisco RPMS Server Administration: Performing Cisco RPMS Administration Tasks, page 3-15
	Port Management	RPMS	Configuring Port Management: Configuring DNIS Groups, page 3-16
			Configuring Port Management: Configuring Trunk Groups, page 3-18
			Configuring Port Management: Understanding Call Types, page 3-19
	Service Level Agreements	RPMS	Configuring Service Level Agreements: Configuring Customer Profiles, page 3-21
			Configuring Service Level Agreements: Configuring Call Discrimination, page 3-22
Configuring Service Level Agreements: Configuring VPDN Services, page 3-24			
Configuring Service Level Agreements: Creating Overflow Pools, page 3-26			
Fault Tolerance	RPMS	Configuring Fault Tolerance: Configuring Cisco RPMS Fault Tolerance, page 3-28	
		Configuring Fault Tolerance: Configuring Fault Tolerance in Cisco RPMS Servers, page 3-30	
		Configuring Fault Tolerance: Configuring Tolerance to an AAA Server Failure, page 3-31	

Table 1-3 As-Needed Operations and Maintenance Tasks (continued)

Managed Component	Subtopic	Tool	Task
Cisco RPMS	Reporting and Accounting	RPMS	Reporting and Accounting: Using Cisco RPMS Reporting, page 3-33
			Reporting and Accounting: Generating Report Types, page 3-34
			Reporting and Accounting: Configuring Accounting, page 3-36
	Troubleshooting		Chapter 16, “Troubleshooting the Cisco RPMS”
Cisco AR	Basic Tasks	CAR	Configuring a Remote Server, page 7-9
			Configuring Session Management, page 7-10
			Checking the AR Server, page 7-11
			Logging in to the Cisco AR, page 7-12
			Configuring, Modifying, and Managing Syslog Messages, page 7-13
			Setting Up and Managing Accounting, page 7-14
			Modifying Configurations Using aregcmd Commands, page 7-15
			Managing the Cisco AR Using aregcmd Commands, page 7-16
			Backing Up the Database, page 7-17
	Troubleshooting		Chapter 14, “Troubleshooting the Cisco Access Registrar”
MIBs	Managing MIBs	IOS	Using MIB Objects, page 8-12

Resource and Network Performance Management

This management category includes not only processing resources, but also performance across the network. This section presents the following topics:

- [Resource Management](#)
- [Network Management](#)
- [Management Tools](#)

Resource Management

When multiple applications are used in the same network, it is important to manage network resources. For example, the Cisco ASAP Solution provides the ability to enforce both network-wide service-level agreements (SLAs) and per-gateway application-overload protection. A universal gateway does not accept a call that violates a network-wide SLA, nor would it consume CPU resources that are in short supply at a given time. This resource management, coupled with hardware and software features, ensures that the availability of applications matches that of the network. For the Cisco ASAP Solution and Cisco PSTN Gateway Solution, Cisco RPMS is used for managing network resources. For information about how to use the Cisco RPMS to manage network resources, refer to [Chapter 3, “Managing Resources and Dial Services: Using Cisco RPMS.”](#)

Network Management

Aside from discovery and inventory management, network management largely implies performance management. The performance of a network can be measured by taking a measurement of response time, line utilization, throughput, and so on. A baseline can be established as a comparison for subsequent performance measurements. Performance levels can be measured to determine whether they are in line with the metrics defined in service-level agreements. This section discusses several aspects of performance management in general, to demonstrate how router performance measurements can be taken and viewed using SNMP (Simple Network Management Protocol).

The tasks involved in performance management include the following:

- Establishing a baseline of network performance
- Defining service-level agreement and metrics
- Monitoring and measuring performance
- Setting thresholds and exception reporting
- Analyzing and tuning

For an in-depth discussion of resource and network management for the ASAP Solution, refer to the *Cisco ASAP Solution Overview and Planning Guide* at the following URL:

<http://www.cisco.com/univercd/cc/td/doc/product/access/solution/asap/index.htm>

Management Tools

Figure 1-1 illustrates the relationship of typical Cisco resource and network management tools to the network components they manage. In the middle layer are, for the most part, element management tools, relying on SNMP for passing messages about the state of components of varying granularity. An exception is Cisco RPMS (Resource Pool Manager Server), which provides resource management to alleviate processing overload and alleviate congestion.



Note

This figure is for illustration only and is not intended to represent all solution architectures. Also, because this document covers the breadth of applications for both the Cisco ASAP Solution and the Cisco SS7 Interconnect for Voice Gateways Solution, it is not expected that you have all the applications that are discussed here, or that you need to manage all the components.

At the bottom are the managed components and their subcomponents. These include Cisco AS5000 series universal gateways (UGs), Cisco 3600 series and Cisco 7200 series H.323 gatekeepers, and the components of the Cisco SC2200 node (also referred to as a Media Gateway Controller [MGC] node). Components of a Cisco SC2200 node include the host platform on which the SS7 signaling software runs, the Cisco 2611 or 2651 Signaling Link Terminals (SLTs), and the Cisco Billing and Measurements Servers (BAMS). These are almost always paired for redundancy. In addition, Cisco Catalyst switches can be considered as being part of a Cisco SC2200 node, although these are not always necessary and can be found in other parts of the network.

Table 1-4 briefly summarizes these Cisco applications, their minimum versions, the components to which they apply, and the solutions they support. The applications are listed in the order in which their chapters appear in this guide. The Cisco ASAP Solution is indicated by *ASAP*, the Cisco SS7 Interconnect for Voice Gateways Solution is indicated by *SS7VG*, and the Cisco PSTN Gateway Solution is indicated by *PSTNGW*.

**Note**

CiscoView, not discussed explicitly in this guide, is a Web-based management tool that provides a graphical view of the Cisco devices at the chassis, card, and port level. It supports all major Cisco devices. UGM and CMNM launch CiscoView. CiscoView also provides management support for the Cisco 5500, and the Cisco SLT (Cisco 2611, Cisco 2651, Cisco AS5400). In addition, Cisco Generic Dial Plan Manager (GDPM) (not discussed explicitly in this guide) helps manage access GWs (Cisco AS5300, Cisco AS5350, Cisco AS5400, Cisco AS5800, and Cisco AS5850).

Table 1-4 Management Applications for Cisco Solutions

Application	Min. Ver. for ASAP	Min. Ver. for PSTNGW	Min. Ver. for SS7VG	Solution Component
Cisco Voice Manager (CVM) (Chapter 2)	2.02	not used	2.02	Cisco 3660 series, Cisco AS5000 series
Cisco RPMS (Chapter 3)	2.0	2.0	not used	Cisco AS5000 series
Cisco Universal Gateway Manager (UGM) (Chapter 4)	2.0	2.1	not used	Cisco AS5000 series
Cisco Media Gateway Manager (CMGM)	not used	2.0	not used	Cisco VISM
Cisco MGC Node Manager (CMNM) (Chapter 5)	1.5	2.3	2.1	Cisco PGW 2200 host, Cisco SC2200 host, Cisco SLT (Cisco 2611, Cisco 2651, or Cisco AS5400), Cisco BAMS, and Cisco Catalyst switch
Cisco Info Center (CIC) (Chapter 6)	3.0	not used	not used	Cisco 3660 series, Cisco AS5000 series, Cisco SC2200 node components
Cisco Access Registrar (AR) (Chapter 7)	1.7	not used	not used	Cisco AS5000 series
Cisco Voice Services Provisioning Tool (VSPT) (Chapter 12)	1.6	2.3	2.2	Cisco SC2200 and Cisco PGW 2200 node components

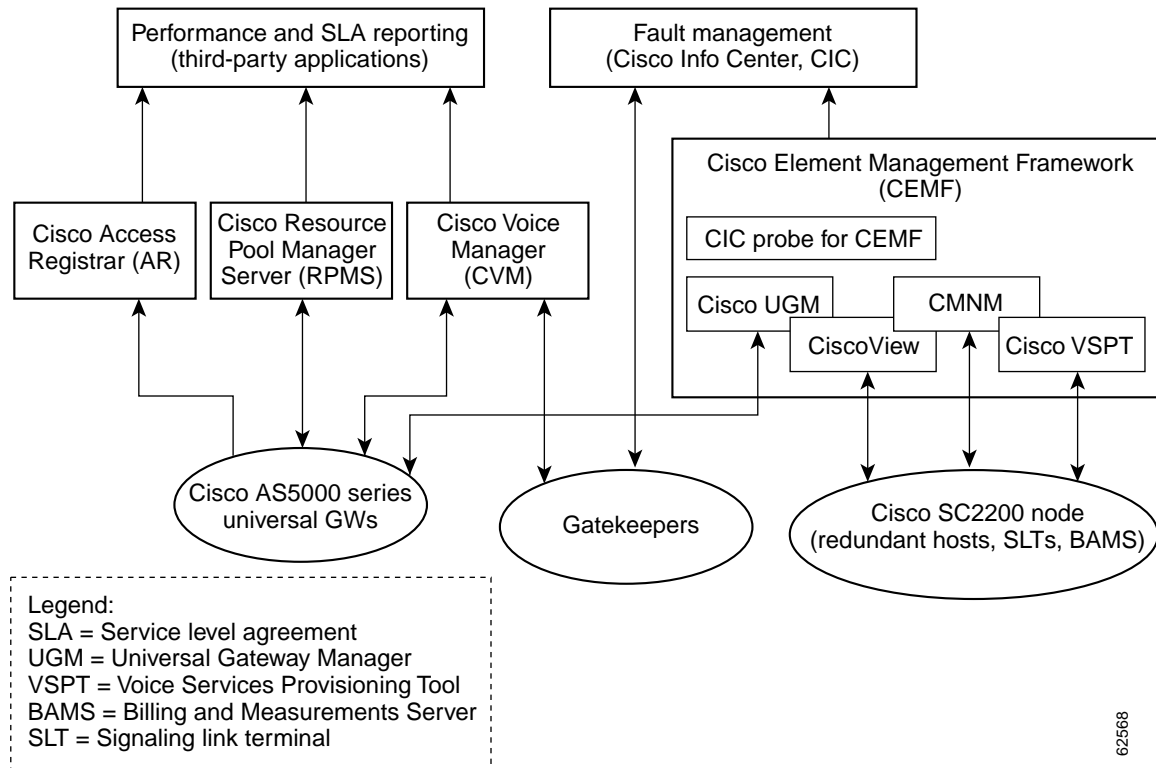
**Note**

For information about the applications and the components of the Cisco ASAP Solution, refer to the *Cisco ASAP Solution Overview and Planning Guide* at the following URL:
<http://www.cisco.com/univercd/cc/td/doc/product/access/solution/asap/index.htm>

**Note**

The foundation for managing the components of a Cisco SC2200 node is the Cisco Element Management Framework (CEMF). Cisco UGM and Cisco Info Center (CIC) also use CEMF. For information on the latest version, refer to Cisco Element Management Framework Release 3.2 at the following URL:
http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cemf/3_2/index.htm

Figure 1-1 Relationship of Resource and Element [Network] Management Applications to Cisco Solution Components



62568

Troubleshooting and Trouble Clearing Tasks: At a Glance

For general internetworking troubleshooting information refer to the *Internetworking Troubleshooting Handbook* at the following URL:

http://www.cisco.com/univercd/cc/td/doc/cisintwk/itg_v1/index.htm

In addition, the following chapters of this guide are dedicated to specific troubleshooting issues:

- Chapter 13, “Troubleshooting SS7 Interconnect Problems: Cisco MGC Node”
- Chapter 14, “Troubleshooting the Cisco Access Registrar”
- Chapter 15, “Troubleshooting Using the Cisco Universal Gateway Manager”
- Chapter 16, “Troubleshooting the Cisco RPMS”



Managing Network Elements and Dial Plans: Using Cisco Voice Manager

Introduction

This chapter presents operations and maintenance tasks related to the Cisco ASAP Solution and the Cisco SS7 Interconnect for Voice Gateways Solution that are provided by the application CiscoWorks2000 Voice Manager (CVM), Release 2.0.2. CVM is part of the CiscoWorks2000 application suite. With this application you can manage network elements, dial plans, and voice ports.



Note

This chapter does not apply to the Cisco PSTN Gateway Solution.

This chapter presents the following major management topics:

- [Managing Network Elements](#)
- [Managing Dial Plans](#)
- [Managing Voice Ports](#)



Tip

See also [Task Summary, page 2-2](#).

Target Platforms

The CiscoWorks2000 Voice Manager application manages the following components of the Cisco ASAP Solution and Cisco SS7 Interconnect for Voice Gateways Solution: Cisco 3660 series and Cisco AS5000 series.

References

For the procedures in this chapter, refer to CiscoWorks2000 Voice Manager 2.0.2 at the following URL:
<http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/voicemgr/cvm2x/cvm202/index.htm>

Windows NT and Sun Solaris of Cisco CVM are available. Depending on your platform, the relevant documents and chapters are either of the following:

- CiscoWorks2000 Voice Manager 2.0 Installation and User Guide for Windows

- Chapter 4, “Using CiscoWorks Voice Manager 2.0 to Manage Devices”
- CiscoWorks2000 Voice Manager 2.0 Installation and User Guide for Solaris
 - Chapter 4, “Using CiscoWorks Voice Manager 2.0 for Solaris to Manage Devices”

Task Summary

The tasks in this chapter are listed below, grouped by major category.

Managing Network Elements

- [Creating, Modifying, and Deleting a UG Group](#)
- [Adding, Modifying, and Deleting a Gatekeeper](#)
- [Creating, Modifying, and Deleting a Local Zone on a GK](#)
- [Creating, Modifying, and Deleting a Remote Zone on a GK](#)
- [Adding, Modifying, Locating, and Deleting a UG](#)
- [Synchronizing Devices](#)
- [Moving a UG](#)
- [Scheduling Tasks](#)

Managing Dial Plans

- [Creating, Modifying, and Deleting a Local Dial Plan](#)
- [Creating, Modifying, and Deleting a Network Dial Plan](#)

Managing Voice Ports

- [Modifying FXO, FXS, E&M, and ISDN Voice Ports](#)

Creating, Modifying, and Deleting a UG Group

Description

Summary	A group is a logical partition of nongatekeeper-managed UGs (routers) that normally interact with each other in a network. Groups must be created in VoIP networks that contain UGs that are not managed by a gatekeeper.
Target Platform(s)	Cisco 3660 series and Cisco AS5000 series
Application	See Introduction, page 2-1
Frequency	As needed

Reference

References depend on your operating system. See [References, page 2-1](#).

Procedure

To create, modify, or delete a UG group:

-
- Step 1** Select the appropriate document and chapter for your operating system.
- Step 2** Read the section Groups.
- Step 3** As appropriate, follow the steps in one or more of the following sections:
- Creating a Group
 - Modifying a Group
 - Deleting a Group
-

Notes

- Related tasks:* [Adding, Modifying, Locating, and Deleting a UG, page 2-7](#)

Adding, Modifying, and Deleting a Gatekeeper

Description

Summary	Gatekeepers (GKs) are used only in VoIP networks and, when added to CVM, they appear only in VoIP view. To add a GK to CVM, you must know the IP addresses and passwords of the GK. This also applies to directory GKs (DGKs), which differ only in their role in the network hierarchy.
Target Platform(s)	Cisco 3660 series and Cisco 7200 series
Application	See Introduction, page 2-1
Frequency	As needed

Reference

References depend on your operating system. See [References, page 2-1](#).

Procedure

To add, modify, or delete a gatekeeper:

-
- Step 1** Select the appropriate document and chapter for your operating system.
- Step 2** Read the section Gatekeepers.
- Step 3** As appropriate, follow the steps in one or more of the following sections:
- a. Adding a Gatekeeper
 - b. Modifying a Gatekeeper
 - c. Deleting a Gatekeeper
-

Notes

- *Related tasks:* [Creating, Modifying, and Deleting a Local Zone on a GK, page 2-5](#), [Creating, Modifying, and Deleting a Remote Zone on a GK, page 2-6](#)
- *Related documents:* For a discussion of H.323 gatekeepers and directory gatekeepers in a VoIP network, refer to Chapter 2, “Provisioning the Gatekeeper Core,” in *Cisco Wholesale Voice Solution Design and Implementation Guide* at the following URL:

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

Creating, Modifying, and Deleting a Local Zone on a GK

Description

Summary	You can create a local zone on a GK after you have added it to CVM.
Target Platform(s)	Cisco 3660 series and Cisco 7200 series
Application	See Introduction, page 2-1
Frequency	As needed

Reference

References depend on your operating system. See [References, page 2-1](#).

Procedure

To create, modify, or delete a local zone on a GK:

-
- Step 1** Select the appropriate document and chapter for your operating system.
- Step 2** Read the section Local Zones.
- Step 3** As appropriate, follow the steps in one or more of the following sections:
- Creating a Local Zone
 - Modifying a Local Zone
 - Deleting a Local Zone
-

Notes

- Related tasks:* [Adding, Modifying, and Deleting a Gatekeeper, page 2-4](#), [Creating, Modifying, and Deleting a Remote Zone on a GK, page 2-6](#)
- Related documents:* See [Notes, page 2-4](#).

Creating, Modifying, and Deleting a Remote Zone on a GK

Description

Summary	You can create a remote zone on a GK after you have added it to CVM.
Target Platform(s)	Cisco 3660 series and Cisco 7200 series
Application	See Introduction, page 2-1
Frequency	As needed

Reference

References depend on your operating system. See [References, page 2-1](#).

Procedure

To create, modify, or delete a remote zone on a GK:

-
- Step 1** Select the appropriate document and chapter for your operating system.
- Step 2** Read the section Remote Zones.
- Step 3** As appropriate, follow the steps in one or more of the following sections:
- a. Creating a Remote Zone
 - b. Modifying a Remote Zone
 - c. Deleting a Remote Zone
-

Notes

- *Related tasks:* [Adding, Modifying, and Deleting a Gatekeeper, page 2-4](#), [Creating, Modifying, and Deleting a Local Zone on a GK, page 2-5](#)
- *Related documents:* For a discussion of H.323 gatekeepers and directory gatekeepers in a VoIP network, refer to Chapter 2, “Provisioning the Gatekeeper Core,” in *Cisco Wholesale Voice Solution Design and Implementation Guide* at the following URL:

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

Adding, Modifying, Locating, and Deleting a UG

Description

Summary	You can manage UGs (which the application terms routers) for combinations of VoIP networks. Groups must be created in VoIP networks that are not managed by a GK.
Target Platform(s)	Cisco AS5000 series
Application	See Introduction, page 2-1
Frequency	As needed

Reference

References depend on your operating system. See [References, page 2-1](#).

Procedure

To add, modify, locate, or delete a UG:

-
- Step 1** Select the appropriate document and chapter for your operating system.
- Step 2** Read the section Routers.
- Step 3** As appropriate, follow the steps in one or more of the following sections:
- Adding a Router
 - Modifying a Router
 - Locating a Router
 - Deleting a Router
-

Notes

- Special issues:* You can also use CVM to save a running configuration. See the section Saving a Running Configuration under the above topics.
- Related tasks:* [Creating, Modifying, and Deleting a UG Group, page 2-3](#)

Synchronizing Devices

Description

Summary	You can synchronize devices (UGs and GKs) to reflect changes you make to voice ports and dial plans through the CLI.
Target Platform(s)	Cisco 3660 series and Cisco AS5000 series
Application	See Introduction, page 2-1
Frequency	As needed

Reference

References depend on your operating system. See [References, page 2-1](#).

Procedure

To synchronize devices:

-
- Step 1** Select the appropriate document and chapter for your operating system.
 - Step 2** Read the section Synchronize Devices.
 - Step 3** As appropriate, follow the steps in one or more of the following sections:
 - a. Synchronize a Router
 - b. Synchronize a Gatekeeper
 - c. Synchronize all Gatekeepers
-

Moving a UG

Description

Summary	You can use drag-and-drop to move a UG in the following modes: between groups, from a group to a GK, from a GK to another GK, and from a GK to a group.
Target Platform(s)	Cisco 3660 series and Cisco AS5000 series
Application	See Introduction, page 2-1
Frequency	As needed

Reference

References depend on your operating system. See [References, page 2-1](#).

Procedure

To move a UG:

-
- | | |
|---------------|--|
| Step 1 | Select the appropriate document and chapter for your operating system. |
| Step 2 | Read the section Moving Routers. |
-

Scheduling Tasks

Description

Summary	With CVM, you can schedule certain tasks to execute at a specific time and date.
Target Platform(s)	Cisco 3660 series and Cisco AS5000 series
Application	See Introduction, page 2-1
Frequency	As needed


Caution

Always take care to schedule network-intensive tasks for off-peak hours.

Reference

References depend on your operating system. See [References, page 2-1](#).

Procedure

To schedule tasks:

-
- Step 1** Select the appropriate document and chapter for your operating system.
 - Step 2** Read the section Scheduling Tasks.
 - Step 3** As appropriate, follow the steps in one or more of the following sections:
 - a. Scheduling a Task
 - b. Rescheduling Tasks
 - c. Deleting a Scheduled Task
-

Creating, Modifying, and Deleting a Local Dial Plan

Description

Summary	You can create, modify, and delete local dial plans (also known as POTS dial plans).
Target Platform(s)	Cisco 3660 series and Cisco AS5000 series
Application	See Introduction, page 2-1
Frequency	As needed

Reference

References depend on your operating system. See [References, page 2-1](#).

Procedure

To create, modify, or delete a local dial plan:

-
- Step 1** Select the appropriate document and chapter for your operating system.
- Step 2** Read the section Local Dial Plans.
- Step 3** As appropriate, follow the steps in one or more of the following sections:
- Creating a Local Dial Plan
 - Modifying a Local Dial Plan
 - Deleting a Local Dial Plan
-

Notes

- Related documents:* Refer to Chapter 4, “Designing a Solution,” in Cisco ASAP Solution Overview and Planning Guide, at the following URL:

http://www.cisco.com/univercd/cc/td/doc/solution/asap_sol/overview/index.htm

Note in particular the section Dial Plans and Number Normalization and the references therein.

Creating, Modifying, and Deleting a Network Dial Plan

Description

Summary	You can create, modify, and delete network VoIP dial plans.
Target Platform(s)	Cisco 3660 series and Cisco AS5000 series
Application	See Introduction, page 2-1
Frequency	As needed



Note

With respect to the Cisco ASAP Solution, you can ignore the discussion of VoFR and VoATM dial plans in the reference pages.

Reference

References depend on your operating system. See [References, page 2-1](#).

Procedure

To create, modify, or delete a network VoIP dial plan:

-
- Step 1** Select the appropriate document and chapter for your operating system.
 - Step 2** Read the section Network Dial Plans.
 - Step 3** As appropriate, follow the steps in one or more of the following sections:
 - a. Creating a VoIP Network Dial Plan
 - b. Modifying a Network Dial Plan
 - c. Deleting a Network Dial Plan
-

Notes

- *Related documents:* Refer to Chapter 4, “Designing a Solution,” in the *Cisco ASAP Solution Overview and Planning Guide* at the following URL:
http://www.cisco.com/univercd/cc/td/doc/solution/asap_sol/overview/index.htm
 Note in particular the section Dial Plans and Number Normalization, and the references therein.

Modifying FXO, FXS, E&M, and ISDN Voice Ports

Description

Summary	You can modify FXO, FXS, E&M, and ISDN voice ports.
Target Platform(s)	Cisco 3660 series and Cisco AS5000 series
Application	See Introduction, page 2-1
Frequency	As needed

Reference

See [References, page 2-1](#).

Procedure

To modify an FXO, FXS, E&M, or ISDN voice port:

-
- Step 1** Select the appropriate document and chapter for your operating system.
- Step 2** Read the section Voice Ports.
- Step 3** As appropriate, follow the steps in one or more of the following sections:
- Modifying an FXO Voice Port
 - Modifying an FXS Voice Port
 - Modifying an E&M Voice Port
 - Modifying an ISDN Voice Port
-

Notes

- Related documents:* A variety of voice port discussions in router documents. See, in particular, *Cisco AS5350 and Cisco AS5400 Universal Gateway Software Configuration Guide* at the following URL: http://www.cisco.com/univercd/cc/td/doc/product/access/acs_serv/as5350/sw_conf/53swcg/



Managing Resources and Dial Services: Using Cisco RPMS

Introduction

This chapter presents operations and maintenance tasks related to the Cisco ASAP Solution *only*, as provided by the application Cisco RPMS, Release 2.0. The main focus is on the Web-based form of the application. However, where CLI commands are applicable, the reader is referred to related commands. CLI commands can be run only on the host machine.



Note

This chapter *does not apply* to the Cisco SS7 Interconnect for Voice Gateways Solution and the Cisco PSTN Gateway Solution only supports RPMS using dial calls.

Tips for troubleshooting Cisco RPMS are provided in [Chapter 16, “Troubleshooting the Cisco RPMS.”](#)



Tip

In some Cisco RPMS documents, “RPMS” may be indicated to stand for “Resource Pool Manager System.” The applications are the same.



Note

The features of Cisco RPMS as they relate to the Cisco ASAP Solution are introduced in the *Cisco ASAP Solution Overview and Planning Guide*.

This chapter presents the following major management topics:

- [Cisco RPMS Server Administration](#)
- [Configuring Port Management](#)
- [Configuring Service Level Agreements](#)
- [Configuring Fault Tolerance](#)
- [Reporting and Accounting](#)



Tip

See also [Task Summary, page 3-2](#).

Target Platforms

The Cisco RPMS application manages the following components of the Cisco ASAP Solution: Cisco AS5000 series.

References

For the following procedures, refer to Cisco Resource Policy Management System 2.0 documentation at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/access/acs_soft/rpms/rpms_2-0/index.htm

The following documents there are referenced:

- *Cisco Resource Policy Management System 2.0 Configuration Guide*
- *Cisco Resource Policy Management System 2.0 Solutions Guide*
- *Cisco Resource Policy Management System 2.0 Wholesale Dial Addendum*

**Note**

For the Cisco RPMS CLI commands, refer to Appendix G, “Using the Command-Line Interface,” of the *Cisco Resource Policy Management System 2.0 Configuration Guide*.

Make sure that you are familiar with the above documents.

Task Summary

The tasks in this chapter are listed below, grouped by major category.

Cisco RPMS Server Administration

- [Cisco RPMS Server Administration: Configuring Cisco RPMS Settings](#)
- [Cisco RPMS Server Administration: Configuring Administrators and Administrators' Privileges](#)
- [Cisco RPMS Server Administration: Configuring Alert Notifications and Logging](#)
- [Cisco RPMS Server Administration: Configuring RADIUS Vendors and VSAs](#)
- [Cisco RPMS Server Administration: Communicating with Universal Gateways](#)
- [Cisco RPMS Server Administration: Configuring AAA Servers](#)
- [Cisco RPMS Server Administration: Configuring SNMP Management](#)
- [Cisco RPMS Server Administration: Resetting Counters](#)
- [Cisco RPMS Server Administration: Managing the Universal Gateway Heartbeat](#)
- [Cisco RPMS Server Administration: Performing Cisco RPMS Administration Tasks](#)

Configuring Port Management

- [Configuring Port Management: Configuring DNIS Groups](#)
- [Configuring Port Management: Configuring Trunk Groups](#)

- [Configuring Port Management: Understanding Call Types](#)

Configuring Service Level Agreements

For information on configuring a Cisco RPMS wholesale dial solution, refer to the *Cisco Resource Policy Management System 2.0 Wholesale Dial Addendum*. For general information, refer to these topics:

- [Configuring Service Level Agreements: Configuring Customer Profiles](#)
- [Configuring Service Level Agreements: Configuring Call Discrimination](#)
- [Configuring Service Level Agreements: Configuring VPDN Services](#)
- [Configuring Service Level Agreements: Creating Overflow Pools](#)

Configuring Fault Tolerance

- [Configuring Fault Tolerance: Configuring Cisco RPMS Fault Tolerance](#)
- [Configuring Fault Tolerance: Configuring Fault Tolerance in Cisco RPMS Servers](#)
- [Configuring Fault Tolerance: Configuring Tolerance to an AAA Server Failure](#)

Reporting and Accounting

- [Reporting and Accounting: Using Cisco RPMS Reporting](#)
- [Reporting and Accounting: Generating Report Types](#)
- [Reporting and Accounting: Configuring Accounting](#)

Cisco RPMS Server Administration: Configuring Cisco RPMS Settings

Description

Summary	You can configure Cisco RPMS settings related to CDRs (Call Data Records), log files, active call times, and threshold settings.
Target Platform(s)	Cisco AS5000 series
Application	See Introduction, page 3-1
Frequency	As needed

Reference

Cisco Resource Policy Management System 2.0 Configuration Guide

For all related documents, see [References, page 3-2](#).

Procedure

To configure Cisco RPMS settings:

-
- | | |
|---------------|--|
| Step 1 | Refer to Chapter 2, “Cisco RPMS Administration,” of the <i>Cisco Resource Policy Management System 2.0 Configuration Guide</i> . |
| Step 2 | Read Overview: Configuring Cisco RPMS Settings. As appropriate, select from among the following options and follow the directions for each option: Call Detail Record Logging and Miscellaneous. |
-

Notes

- *Related documents:* Call Detail Records in Chapter 2, “Cisco RPMS Features,” of the *Cisco Resource Policy Management System 2.0 Solutions Guide*.

Cisco RPMS Server Administration: Configuring Administrators and Administrators' Privileges

Description

Summary	Cisco RPMS supports multiple administrators with different privilege levels.
Target Platform(s)	Cisco AS5000 series
Application	See Introduction, page 3-1
Frequency	As needed

Reference

Cisco Resource Policy Management System 2.0 Configuration Guide

For all related documents, see [References, page 3-2](#).

Procedure

To add administrators and select a privilege level:

-
- | | |
|---------------|--|
| Step 1 | Refer to Chapter 2, “Cisco RPMS Administration,” of the <i>Cisco Resource Policy Management System 2.0 Configuration Guide</i> . |
| Step 2 | Read Overview: Configuring Administrators and Administrators' Privileges and follow the steps therein. |
| Step 3 | Select privilege levels as appropriate. |
-

Notes

- *Related tasks:*
 - Adding an Administrator
 - Editing an Administrator
 - Deleting an Administrator
- *Related documents:* User Administration in Chapter 2, “Cisco RPMS Features,” of the *Cisco Resource Policy Management System 2.0 Solutions Guide*

Cisco RPMS Server Administration: Configuring Alert Notifications and Logging

Description

Summary	You can configure Cisco RPMS to send e-mail notifications when alerts occur. You can also enable alert logging.
Target Platform(s)	Cisco AS5000 series
Application	See Introduction, page 3-1
Frequency	As needed

Reference

Cisco Resource Policy Management System 2.0 Configuration Guide

For all related documents, see [References, page 3-2](#).

Procedure

To configure alert notifications or enable alert logging:

-
- Step 1** Refer to Chapter 2, “Cisco RPMS Administration” of the *Cisco Resource Policy Management System 2.0 Configuration Guide*.
- Step 2** Read Overview: Configuring Alert Notifications and follow the steps for each of the following tasks, as appropriate:
- Configuring the Email Server and Sender Email Address
 - Adding Email Addresses to Receive Notifications
 - Enabling Alert Logging
-

Notes

- Related documents:* Alerts in Chapter 2, “Cisco RPMS Features,” of the *Cisco Resource Policy Management System 2.0 Solutions Guide*

Cisco RPMS Server Administration: Configuring RADIUS Vendors and VSAs

Description

Summary	Cisco Vendor Specific Attributes (VSAs) are sent in the preauthentication “accept” message from Cisco RPMS to direct the UG how to handle the call. Cisco RPMS provides a Web-based interface to (1) define a vendor (specific RADIUS application type), and (2) administer and associate any VSA with a customer-based call-accept message. This increases control over resources and service management for each call.
Target Platform(s)	Cisco AS5000 series
Application	See Introduction, page 3-1
Frequency	As needed

Reference

Cisco Resource Policy Management System 2.0 Configuration Guide

For all related documents, see [References, page 3-2](#).

Procedure

To configure a RADIUS vendor and VSAs:

-
- | | |
|---------------|--|
| Step 1 | Refer to Chapter 2, “Cisco RPMS Administration,” of the <i>Cisco Resource Policy Management System 2.0 Configuration Guide</i> . |
| Step 2 | Read Overview: Configuring RADIUS Vendors and follow the steps for each of the following tasks, as appropriate: <ol style="list-style-type: none">Adding a RADIUS VendorEditing a VendorDeleting a VendorEditing a Vendor Specific AttributeDeleting a Vendor Specific AttributeAssociating a Vendor Specific Attribute to a Customer Profile |
-

Notes

- *Special issues:* Both VSA strings must be configured for the authentication type to be applied on the UG. Using an incorrect argument syntax for the **auth-type** field may cause calls to fail to authenticate, and therefore disconnect.
- *Related tasks:*
 - Viewing a Vendor
 - Viewing a Vendor Specific Attribute
 - Building Vendor Specific Attributes for Modem Management
 - Building Vendor Specific Attributes to Control Authentication Type
 - Editing a Vendor Specific Attribute in a Customer Profile
 - Deleting a Vendor Specific Attribute from a Customer Profile
- *Related documents:*
 - Chapter 6, “Cisco RPMS Building Blocks,” of the *Cisco Resource Policy Management System 2.0 Solutions Guide*
 - Configuring AAA Preauthentication, under “Security Server Protocols—Configuring Radius” in the *Cisco IOS Security Configuration Guide, Release 12.2*

Cisco RPMS Server Administration: Communicating with Universal Gateways

Description

Summary	Cisco RPMS and UGs communicate by using the RADIUS protocol. You can create a list of UGs that communicate with Cisco RPMS.
Target Platform(s)	Cisco AS5000 series
Application	See Introduction, page 3-1
Frequency	As needed

Reference

Cisco Resource Policy Management System 2.0 Configuration Guide

For all related documents, see [References, page 3-2](#).

Procedure

To add UGs that communicate with Cisco RPMS:

-
- | | |
|---------------|--|
| Step 1 | Refer to Chapter 2, “Cisco RPMS Administration,” of the <i>Cisco Resource Policy Management System 2.0 Configuration Guide</i> . |
| Step 2 | Read Overview: Communicating with Universal Gateways and follow the steps to add a UG. |
-

Notes

- *Special issues:*
 - You must configure universal gateways to communicate with Cisco RPMS.
 - Ascend translators do not support VPDN features.
- *Related tasks:* none
- *Related documents:*
 - Appendix A, “Configuring the Universal Gateway,” of the *Cisco Resource Policy Management System 2.0 Configuration Guide*
 - Appendix A, “Helpful Links,” of the *Cisco Resource Policy Management System 2.0 Solutions Guide*

Cisco RPMS Server Administration: Configuring AAA Servers

Description

Summary	The UG can be provisioned to communicate with a list of AAA RADIUS servers. The use of proxy servers for redundancy provides fault tolerance in case one server is unreachable—the UG can redirect traffic to another RADIUS server in the list.
Target Platform(s)	Cisco AS5000 series
Application	See Introduction, page 3-1
Frequency	As needed

Reference

Cisco Resource Policy Management System 2.0 Configuration Guide

For all related documents, see [References, page 3-2](#).

Procedure

To configure AAA servers or AAA proxy servers:

-
- | | |
|---------------|--|
| Step 1 | Refer to Chapter 2, “Cisco RPMS Administration,” of the <i>Cisco Resource Policy Management System 2.0 Configuration Guide</i> . |
| Step 2 | Read Overview: AAA Servers and follow the steps therein. |
-

Notes

- *Special issues:* Although AAA proxy servers are optional components, Cisco recommends using them in your deployment.
- *Related documents:*
 - Appendix B, “Configuring Access Registrar,” of the *Cisco Resource Policy Management System 2.0 Configuration Guide*
 - Chapter 4, “Fault Tolerance,” of the *Cisco Resource Policy Management System 2.0 Solutions Guide*
 - Chapter 5, “Cisco RPMS Deployment Scenarios,” of the *Cisco Resource Policy Management System 2.0 Solutions Guide*

Cisco RPMS Server Administration: Configuring SNMP Management

Description

Summary	Cisco RPMS includes an SNMP agent to monitor Cisco RPMS state information. The Cisco RPMS state information includes attributes such as system up time, customer profiles, and VPDN group information and statistics.
Target Platform(s)	Cisco AS5000 series
Application	See Introduction, page 3-1
Frequency	As needed

Reference

Cisco Resource Policy Management System 2.0 Configuration Guide

For all related documents, see [References, page 3-2](#).

Procedure

To configure SNMP management:

-
- | | |
|---------------|--|
| Step 1 | Refer to Chapter 2, “Cisco RPMS Administration,” of the <i>Cisco Resource Policy Management System 2.0 Configuration Guide</i> . |
| Step 2 | Read Overview: SNMP Management and follow the steps therein. |
-

Notes

- *Related tasks:*
 - Configuring the SNMP Agent
 - Adding an SNMP Manager Host
 - Adding an SNMP Trap Manager Host
- *Related documents:* Overview: SNMP Support in Chapter 2, “Cisco RPMS Features,” of the *Cisco Resource Policy Management System 2.0 Solutions Guide*

Cisco RPMS Server Administration: Resetting Counters

Description

Summary	Cisco RPMS uses two types of counters that can be reset: system counters and informational counters. <i>System counters</i> help manage and maintain session counts on the UGs, directly affecting port management decisions and thresholds. <i>Informational counters</i> increment until they are reset. These maintain information on rejected sessions, rejected VPDN sessions, and sessions that were rejected because of insufficient resources.
Target Platform(s)	Cisco AS5000 series
Application	See Introduction, page 3-1
Frequency	As needed

Reference

Cisco Resource Policy Management System 2.0 Configuration Guide

For all related documents, see [References, page 3-2](#).

Procedure

To reset system or informational counters:

-
- | | |
|---------------|--|
| Step 1 | Refer to Chapter 2, “Cisco RPMS Administration,” of the <i>Cisco Resource Policy Management System 2.0 Configuration Guide</i> . |
| Step 2 | Read Overview: Counters and reset system or informational counters, as appropriate. |
-

Notes

- *Special issues:* Resetting system counters can cause the Cisco RPMS counters to become out of sync with the counters on the managed UGs.
- *Related documents:* Overview: Resetting Counters in Chapter 6, “Reporting and Accounting,” of the *Cisco Resource Policy Management System 2.0 Configuration Guide*

Cisco RPMS Server Administration: Managing the Universal Gateway Heartbeat

Description

Summary	Cisco RPMS can monitor the UG's state. If a UG fails to respond to an SNMP Get message or cannot be reached by means of ICMP, Cisco RPMS resets the corresponding active calls.
Target Platform(s)	Cisco AS5000 series
Application	See Introduction, page 3-1
Frequency	As needed

Reference

Cisco Resource Policy Management System 2.0 Configuration Guide

For all related documents, see [References, page 3-2](#).

Procedure

To manage UG heartbeat:

-
- | | |
|---------------|--|
| Step 1 | Refer to Chapter 2, "Cisco RPMS Administration," of the <i>Cisco Resource Policy Management System 2.0 Configuration Guide</i> . |
| Step 2 | Read Overview: The Universal Gateway Heartbeat and follow the steps therein. |
-

Notes

- *Related documents:* Detection of Universal Gateway Failure in Chapter 4, "Fault Tolerance," of the *Cisco Resource Policy Management System 2.0 Solutions Guide*

Cisco RPMS Server Administration: Performing Cisco RPMS Administration Tasks

Description

Summary	There are a variety of options for configuring administration tasks in Cisco RPMS.
Target Platform(s)	Cisco AS5000 series
Application	See Introduction , page 3-1
Frequency	As needed

Reference

Cisco Resource Policy Management System 2.0 Configuration Guide

For all related documents, see [References](#), page 3-2.

Procedure

To configure Cisco RPMS administration tasks:

-
- | | |
|---------------|--|
| Step 1 | Refer to Chapter 2, “Cisco RPMS Administration,” of the <i>Cisco Resource Policy Management System 2.0 Configuration Guide</i> . |
| Step 2 | Read Overview: Cisco RPMS Administration Tasks and configure the appropriate tasks. |
-

Notes

- *Related tasks:*
 - Starting and Stopping Cisco RPMS
 - Starting and Stopping Individual Components of Cisco RPMS
 - Connecting to a Remote Cisco RPMS Server
 - Defining Cisco RPMS Configuration Files
 - Logging and Debugging
 - Managing the Log File Directory
 - Managing the Call Detail Record directory
- *Related documents:* *Cisco Resource Policy Management System 2.0 Solutions Guide*

Configuring Port Management: Configuring DNIS Groups

Description

Summary	A DNIS group is a configured list of DNIS numbers corresponding to the numbers dialed by particular customers, service offerings, or both. Cisco RPMS checks the DNIS number of inbound calls against the configured DNIS groups or the default DNIS group. If a match is found, the configured information in the customer profile to which the DNIS group is assigned is used. If a match is not found, the default DNIS group and default customer profile are used. If a default customer profile is not configured, the call is rejected.
Target Platform(s)	Cisco AS5000 series
Application	See Introduction, page 3-1
Frequency	As needed

Reference

Cisco Resource Policy Management System 2.0 Configuration Guide

For all related documents, see [References, page 3-2](#).

Procedures

To configure a DNIS group, complete the following tasks:

-
- | | |
|---------------|---|
| Step 1 | Refer to Chapter 3, “Configuring Core Service Level Agreement Building Blocks,” of the <i>Cisco Resource Policy Management System 2.0 Configuration Guide</i> . |
| Step 2 | Read Overview: Configuring DNIS Groups and follow the steps therein. |
-

Notes

- *Related tasks:*
 - Creating a DNIS Group
 - Adding a DNIS Number to a DNIS Group
 - Editing a DNIS Group
 - Editing a DNIS Number
 - Deleting a DNIS Group
 - Deleting a DNIS Number
- *Related documents:* The DNIS Groups and Customer Profile sections in Chapter 6, “Cisco RPMS Building Blocks,” of the *Cisco Resource Policy Management System 2.0 Solutions Guide*

Configuring Port Management: Configuring Trunk Groups

Description

Summary	Trunk groups contain a list of trunks that belong to a customer. Both trunks and trunk groups allow Cisco RPMS users to manage multiple calls from different areas, by using more than one customer profile.
Target Platform(s)	Cisco AS5000 series
Application	See Introduction, page 3-1
Frequency	As needed

Reference

Cisco Resource Policy Management System 2.0 Configuration Guide

For all related documents, see [References, page 3-2](#).

Procedures

To configure trunk groups, complete the following tasks:

-
- | | |
|---------------|---|
| Step 1 | Refer to Chapter 3, “Configuring Core Service Level Agreement Building Blocks,” of the <i>Cisco Resource Policy Management System 2.0 Configuration Guide</i> . |
| Step 2 | Read Overview: Configuring Trunk Groups and follow the steps therein. |
-

Notes

- *Related tasks:*
 - Creating a Trunk Group
 - Adding Trunks to the Trunk Group
 - Associating the Trunk Group
 - Editing a Trunk
 - Deleting a Trunk Group
 - Deleting a Trunk
- *Related documents:* The Trunk Groups and Customer Profile sections in Chapter 6, “Cisco RPMS Building Blocks,” of the *Cisco Resource Policy Management System 2.0 Solutions Guide*

Configuring Port Management: Understanding Call Types

Description

Summary	Customer profiles use call types to identify which default customer profile to use for an incoming call. For DNIS groups, when multiple default customer profiles are used, the call type of the DNIS group identifies which default customer profile to use for an incoming call.
Target Platform(s)	Cisco AS5000 series
Application	See Introduction, page 3-1
Frequency	As needed

Reference

Cisco Resource Policy Management System 2.0 Configuration Guide

For all related documents, see [References, page 3-2](#).

Procedure

To read about call types, complete the following tasks:

-
- | | |
|---------------|---|
| Step 1 | Refer to Chapter 3, “Configuring Core Service Level Agreement Building Blocks,” of the <i>Cisco Resource Policy Management System 2.0 Configuration Guide</i> . |
| Step 2 | Read Overview: Call Types. |
-

Notes

- *Related tasks:*
 - Configuring a Customer Profile
 - Configuring a DNIS Group
 - Call Types
- *Related documents:*
 - Call Types in Chapter 6, “Cisco RPMS Building Blocks,” of the *Cisco Resource Policy Management System 2.0 Solution Guide*
 - Configuring Customer Profiles in Chapter 4, “Building Service Level Agreements,” of the *Cisco Resource Policy Management System 2.0 Configuration Guide*

Configuring Service Level Agreements: Configuring Customer Profiles

Description

Summary	<p>A customer profile is a set of parameters created for a specific service provider customer. The parameters are configured by the Cisco RPMS administrator and are based on the DNIS and call types.</p> <p>You can assign configured DNIS groups, trunk groups, and IP groups to customer profiles. The customer profiles are selected by matching the incoming call characteristics (DNIS, call type, trunk) with the combinations of the entries within these associated groups.</p>
Target Platform(s)	Cisco AS5000 series
Application	See Introduction, page 3-1
Frequency	As needed

Reference

Cisco Resource Policy Management System 2.0 Configuration Guide

For all related documents, see [References, page 3-2](#).

Procedure

To configure a customer profile, complete the following tasks:

-
- | | |
|---------------|--|
| Step 1 | Refer to Chapter 4, “Building Service Level Agreements,” of the <i>Cisco Resource Policy Management System 2.0 Configuration Guide</i> . |
| Step 2 | Read Overview: Configuring Customer Profiles and follow the steps therein. |
-

Notes

- *Related tasks:*
 - Configuring a DNIS Group
 - Configuring Trunk Groups
- *Related documents:* Configuring Customer Profiles in Chapter 4, “Building Service Level Agreements,” of the *Cisco Resource Policy Management System 2.0 Configuration Guide*

Configuring Service Level Agreements: Configuring Call Discrimination

Description

Summary	Call discrimination uses DNIS groups to prevent specific call types from accessing resources on the UGs. For example, if a customer signs up for modem access, you can prevent that customer from accessing the UG through ISDN by creating a table entry that prevents digital access for the customer's DNIS group.
Target Platform(s)	Cisco AS5000 series
Application	See Introduction, page 3-1
Frequency	As needed

Reference

Cisco Resource Policy Management System 2.0 Configuration Guide

For all related documents, see [References, page 3-2](#).

Procedure

To configure call discrimination, complete the following tasks:

-
- | | |
|---------------|--|
| Step 1 | Refer to Chapter 4, “Building Service Level Agreements,” of the <i>Cisco Resource Policy Management System 2.0 Configuration Guide</i> . |
| Step 2 | Read Overview: Configuring Call Discrimination and follow the steps therein. |
-

Notes

- *Special issues:*
 - Cisco RPMS Call Discrimination Table entry names are case sensitive.
 - If a call type is not available in a RADIUS message, Cisco RPMS uses a call type of *any*.
- *Related tasks:*
 - Creating Call Discrimination
 - Viewing Call Discrimination
 - Editing Call Discrimination
 - Deleting Call Discrimination
- *Related documents:* Call Discrimination in Chapter 6, “Cisco RPMS Building Blocks,” of the *Cisco Resource Policy Management System 2.0 Solutions Guide*

Configuring Service Level Agreements: Configuring VPDN Services

Description

Summary	If the UG is configured for VPDN service, it sends a request to Cisco RPMS for VPDN information after answering a call. Cisco RPMS determines whether to authenticate the call with a home gateway through a VPDN tunnel based on the type of VPDN services configured in Cisco RPMS. Cisco RPMS supports the following types of VPDN services: <ul style="list-style-type: none">• DNIS-based VPDN dial service• Domain name-based VPDN dial service• VPDN request forwarding to external AAA server
Target Platform(s)	Cisco AS5000 series
Application	See Introduction, page 3-1
Frequency	As needed

Reference

Cisco Resource Policy Management System 2.0 Configuration Guide

For all related documents, see [References, page 3-2](#).

Procedure

To configure VPDN services, follow the steps in one or more of the following sections as appropriate:

-
- | | |
|---------------|--|
| Step 1 | Refer to Chapter 4, “Building Service Level Agreements,” of the <i>Cisco Resource Policy Management System 2.0 Configuration Guide</i> . |
| Step 2 | Read Overview: Configuring VPDN Services. |
| Step 3 | If configuring DNIS-based VPDN, read Overview: DNIS-Based VPDN. |
| Step 4 | If configuring domain name-based VPDN, read Overview: Domain Name-Based VPDN. |
| Step 5 | If configuring VPDN request forwarding, read Overview: VPDN Request Forwarding to External AAA Server. |
-

Notes

- *Related documents:*
 - Read the VPDN and VPDN Group sections of Chapter 6, “Cisco RPMS Building Blocks,” of the *Cisco Resource Policy Management System 2.0 Solutions Guide*.
 - Refer to *Cisco Resource Policy Management System 2.0 Wholesale Dial Addendum* for information on provisioning a wholesale dial network with VPDN.

Configuring Service Level Agreements: Creating Overflow Pools

Description

Summary	With Cisco RPMS, you can control overflow access through shared overflow pools. To create an overflow pool, you must give it a name, and then associate one or more trunk groups to it.
Target Platform(s)	Cisco AS5000 series
Application	See Introduction, page 3-1
Frequency	As needed

Reference

Cisco Resource Policy Management System 2.0 Configuration Guide

For all related documents, see [References, page 3-2](#).

Procedures

To create an overflow pool, complete the following tasks:

-
- | | |
|---------------|--|
| Step 1 | Refer to Chapter 4, “Building Service Level Agreements,” of the <i>Cisco Resource Policy Management System 2.0 Configuration Guide</i> . |
| Step 2 | Read Overview: Configuring Overflow Pools. |
-

Notes

- *Special issues:*
 - A trunk group cannot be associated to more than one overflow pool.
 - An overflow call is a call received when the session count limit has been exceeded and is in an overflow state. When a call is identified as an overflow call, it maintains overflow status throughout its duration, even if the number of current sessions falls below the session count limit.
- *Related tasks:*
 - Creating an Overflow Pool
 - Adding a Trunk Group to an Overflow Pool
 - Adding Service Type Limits to an Overflow Pool
 - Viewing an Overflow Pool
 - Editing an Overflow Pool
 - Deleting an Overflow Pool
 - Deleting a Trunk Group from an Overflow Pool
 - Deleting a Service Type Limit from an Overflow Pool
- *Related documents:* Overflow Pools in Chapter 6, “Cisco RPMS Building Blocks,” of the *Cisco Resource Policy Management System 2.0 Solutions Guide*

Configuring Fault Tolerance: Configuring Cisco RPMS Fault Tolerance

Description

Summary	Cisco RPMS allows you to build fault tolerance and resiliency into your dial service offerings.
Target Platform(s)	Cisco AS5000 series
Application	See Introduction, page 3-1
Frequency	As needed

Reference

Cisco Resource Policy Management System 2.0 Configuration Guide

For all related documents, see [References, page 3-2](#).

Procedure

To configure Cisco RPMS fault tolerance:

-
- | | |
|---------------|--|
| Step 1 | Refer to Chapter 5, “Configuring Cisco RPMS Fault Tolerance,” of the <i>Cisco Resource Policy Management System 2.0 Configuration Guide</i> . |
| Step 2 | Read Overview: Configuring Cisco RPMS Fault Tolerance. |
| Step 3 | As appropriate, follow the steps in one or more of the following sections: <ul style="list-style-type: none">• Hot Standby• Tolerance to Database Failures• Cisco RPMS Autorestart• Detection of Universal Gateway Failures |
-

Notes

- *Related tasks:*
 - Tolerance to Cisco RPMS Server Failure
 - Tolerance to AAA Server Failure
- *Related documents:* Chapter 4, “Fault Tolerance,” of the *Cisco Resource Policy Management System 2.0 Solutions Guide*

Configuring Fault Tolerance: Configuring Fault Tolerance in Cisco RPMS Servers

Description

Summary	To enhance fault tolerance in case of a server failure, configure Cisco RPMS servers as hot standby pairs. The pairs communicate with each other and constantly share information. By remaining in synchronization, both servers in a hot standby pair always have identical active call counts and other network state information. You can also configure Cisco RPMS proxies, to use one server as an active server and the other as a standby server.
Target Platform(s)	Cisco AS5000 series
Application	See Introduction, page 3-1
Frequency	As needed

Reference

Cisco Resource Policy Management System 2.0 Configuration Guide

For all related documents, see [References, page 3-2](#).

Procedure

To configure fault tolerance in Cisco RPMS servers, complete the following tasks:

-
- | | |
|---------------|--|
| Step 1 | Refer to Chapter 5, “Configuring Cisco RPMS Fault Tolerance,” of the <i>Cisco Resource Policy Management System 2.0 Configuration Guide</i> . |
| Step 2 | Read the Overview: Tolerance to Cisco RPMS Server Failure. |
| Step 3 | As appropriate, follow the steps in one or more of the following sections: <ol style="list-style-type: none"> a. Configuring a Hot Standby Pair b. Configuring the Cisco RPMS Proxy for Failover to the Standby Server |
-

Notes

- *Related documents:* Chapter 4, “Fault Tolerance,” in the *Cisco Resource Policy Management System 2.0 Solutions Guide*

Configuring Fault Tolerance: Configuring Tolerance to an AAA Server Failure

Description

Summary	To enhance fault tolerance in case of an AAA server failure, Cisco RPMS allows you to create a prioritized list of AAA servers. Cisco RPMS proxies use this list to determine the destination of authorization and accounting messages received from the UG. The proxies forward messages to the AAA server with the highest priority. If they detect that this AAA server has failed, they switch over to the server with the next highest priority.
Target Platform(s)	Cisco AS5000 series
Application	See Introduction, page 3-1
Frequency	As needed

Reference

Cisco Resource Policy Management System 2.0 Configuration Guide

For all related documents, see [References, page 3-2](#).

Procedure

To configure tolerance to AAA server failure:

-
- | | |
|---------------|---|
| Step 1 | Refer to Chapter 5, “Configuring Cisco RPMS Fault Tolerance,” of the <i>Cisco Resource Policy Management System 2.0 Configuration Guide</i> . |
| Step 2 | Read Overview: Tolerance to AAA Server Failure and follow the steps therein. |
-

Notes

- *Related tasks:* Configuring the AAA Server
- *Related documents:*
 - Appendix B, “Configuring Access Registrar,” of the *Cisco Resource Policy Management System 2.0 Configuration Guide*
 - Adding a AAA Server or AAA Proxy Server in Chapter 2, “Cisco RPMS Administration,” of the *Cisco Resource Policy Management System 2.0 Configuration Guide*
 - Overview: Tolerance to Cisco RPMS Server Failure in Chapter 2, “Cisco RPMS Administration,” of the *Cisco Resource Policy Management System 2.0 Configuration Guide*

Reporting and Accounting: Using Cisco RPMS Reporting

Description

Summary	Cisco RPMS reports data for network dial service analysis and troubleshooting. Various types of reports can be generated for different purposes.
Target Platform(s)	Cisco AS5000 series
Application	See Introduction, page 3-1 .
Frequency	As needed.

Reference

Cisco Resource Policy Management System 2.0 Configuration Guide

For all related documents, see [References, page 3-2](#).

Procedure

To view or edit Cisco RPMS reports:

-
- | | |
|---------------|---|
| Step 1 | Refer to Chapter 6, “Reporting and Accounting,” of the <i>Cisco Resource Policy Management System 2.0 Configuration Guide</i> . |
| Step 2 | Read Overview: Report Types. |
-

Notes

- *Related tasks:*
 - Viewing Reports
 - Editing a Report Layout
 - Filtering a Report
- *Related documents:* Overview: Reports in Chapter 6, “Cisco RPMS Building Blocks,” of the *Cisco Resource Policy Management System 2.0 Solutions Guide*

Reporting and Accounting: Generating Report Types

Description

Summary You can generate reports on the following topics:

- Customer Profile Report
- DNIS Report
- DNIS Group Report
- Domain Name Report
- IP Endpoints Report
- Tunnel Report
- VPDN Group Report
- Recent Call Report
- Overflow Pool Report

Target Platform(s) Cisco AS5000 series

Application See [Introduction, page 3-1](#).

Frequency As needed.

Reference

Cisco Resource Policy Management System 2.0 Configuration Guide

For all related documents, see [References, page 3-2](#).

Procedure

To generate various Cisco RPMS reports:

Step 1 Refer to Chapter 6, “Reporting and Accounting,” of the *Cisco Resource Policy Management System 2.0 Configuration Guide*.

Step 2 Read Overview: Report Types and select the appropriate report types.

Notes

- *Related documents:* Overview: Reports in Chapter 6, “Cisco RPMS Building Blocks,” of the *Cisco Resource Policy Management System 2.0 Solutions Guide*

Reporting and Accounting: Configuring Accounting

Description

Summary	Accounting allows you to specify where Cisco RPMS forwards messages, and to generate Call Detail Records (CDRs).
Target Platform(s)	Cisco AS5000 series
Application	See Introduction, page 3-1
Frequency	As needed

Reference

Cisco Resource Policy Management System 2.0 Configuration Guide

For all related documents, see [References, page 3-2](#).

Procedure

To configure accounting:

-
- | | |
|---------------|---|
| Step 1 | Refer to Chapter 6, “Reporting and Accounting,” of the <i>Cisco Resource Policy Management System 2.0 Configuration Guide</i> . |
| Step 2 | Read Overview: Accounting and follow the steps therein. |
-

Notes

- *Related documents:* Accounting and Billing Support in Chapter 2, “Cisco RPMS Features,” of the *Cisco Resource Policy Management System 2.0 Solutions Guide*



Managing Network Objects: Using Cisco UGM

Introduction

This chapter presents operations and maintenance tasks related to the Cisco ASAP Solution and Cisco PSTN Gateway Solution, as provided by the application Cisco Universal Gateway Manager (Cisco UGM), Release 2.



Note

This chapter *does not apply* to the Cisco SS7 Interconnect for Voice Gateways Solution.

Tips for troubleshooting solution components and networks by means of Cisco UGM are provided in [Chapter 15, “Troubleshooting Using the Cisco Universal Gateway Manager.”](#)



Note

The features of Cisco UGM as they relate to the Cisco ASAP Solution are introduced in the *Cisco ASAP Solution Overview and Planning Guide*.

For the tasks presented in this chapter, see [Task Summary, page 4-2](#).

Target Platforms

The Cisco UGM application manages the following components of the Cisco ASAP Solution and Cisco PSTN Gateway Solution:

- Cisco AS5300
- Cisco AS5350
- Cisco AS5400
- Cisco AS5800
- Cisco AS5850.

Support for redundancy and high availability is provided for the Cisco AS5800 and Cisco AS5850.

References

The Cisco UGM documentation, including a user's guide, a quick guide, and release notes, can be found at the following URL:

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



Note For the step-by-step procedures for doing the tasks listed below, refer to the *Cisco Universal Gateway Manager Users Guide, Version 2.0*.

Refer also to the *Cisco Element Management Framework User Guide*. The most current version of the Cisco Element Management Framework (CEMF) documentation can be found at the following URL:

<http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cemf/index.htm>

Task Summary

The tasks in this chapter are listed below.

- [Deploying and Discovering Network Objects](#)
- [Managing and Exporting Inventory Data](#)
- [Managing Redundancy and High Availability](#)
- [Configuring Managed Devices](#)
- [Managing Images and Scheduling Actions](#)
- [Configuring the Administrative State of Objects](#)
- [Managing Security on Cisco UGM-Managed Devices](#)
- [Managing Device Performance](#)
- [Managing Faults](#)
- [Managing Presence Polling and Loss of Communication](#)

Deploying and Discovering Network Objects

Description

Summary	Before you can use Cisco UGM to manage devices, you must first create new “objects” that represent real managed network elements. Managed devices are represented by device objects, and the cards and ports in the device are represented by device component objects.
Target Platform(s)	Cisco AS5300, Cisco AS5350, Cisco AS5400, Cisco AS5800, Cisco AS5850
Application	See Introduction, page 4-1
Frequency	As needed

Reference

Cisco Universal Gateway Manager Users Guide, Version 2.0

For all related documents, see [References, page 4-2](#).

Procedure

To deploy a region or site object automatically:

-
- | | |
|---------------|--|
| Step 1 | In the above reference, refer to Chapter 1, “Deploying, Discovering, and Exporting Inventory Data with Cisco UGM.” |
| Step 2 | Read the section Overview of Deployment and Discovery. |
| Step 3 | As appropriate, read the introductory material and follow the steps in one or more of the following sections: <ul style="list-style-type: none">a. Deploying Region, Site, or Bay Container Objectsb. Deploying Device Objects Manuallyc. Auto Discovering Device Objectsd. Auto Discovering Device Component Objects |
-

Managing and Exporting Inventory Data

Description

Summary	You can export your inventory data to a flat text file. With report-generating software you can format the data into a report. There are also data-management options.
Target Platform(s)	Cisco AS5300, Cisco AS5350, Cisco AS5400, Cisco AS5800, Cisco AS5850
Application	See Introduction, page 4-1
Frequency	As needed

Reference

Cisco Universal Gateway Manager Users Guide, Version 2.0

For all related documents, see [References, page 4-2](#).

Procedure

To manage and export inventory data:

-
- | | |
|---------------|---|
| Step 1 | In the above reference, refer to Chapter 1, “Deploying, Discovering, and Exporting Inventory Data with Cisco UGM.” |
| Step 2 | Read the section Overview of Exporting Inventory Data. |
| Step 3 | As appropriate, read the introductory material and follow the steps in one or more of the following sections: <ol style="list-style-type: none">Updating Inventory DataExporting Inventory Data ImmediatelyScheduling Inventory Data Export |
-

Managing Redundancy and High Availability

Description

Summary	Cisco UGM supports redundancy in Cisco AS5800 platforms, and high availability (HA) in Cisco AS5850 platforms.
Target Platform(s)	Cisco AS5800, Cisco AS5850
Application	See Introduction, page 4-1
Frequency	As needed

Reference

Cisco Universal Gateway Manager Users Guide, Version 2.0

For all related documents, see [References, page 4-2](#).

Procedure

To manage redundancy in Cisco AS5800 platforms and high availability in Cisco AS5850 platforms:

-
- | | |
|---------------|---|
| Step 1 | In the above reference, refer to Chapter 1, “Deploying, Discovering, and Exporting Inventory Data with Cisco UGM.” |
| Step 2 | As appropriate, read the section Overview of Redundancy and High Availability Support and follow the recommendations therein. |
-

Configuring Managed Devices

Description

Summary	Because many users can access Cisco UGM, you must prevent multiple users from simultaneously accessing and modifying a network object or any of its components. This requires establishing access schedules for all users.
Target Platform(s)	Cisco AS5300, Cisco AS5350, Cisco AS5400, Cisco AS5800, Cisco AS5850
Application	See Introduction, page 4-1
Frequency	As needed

Reference

Cisco Universal Gateway Manager Users Guide, Version 2.0

For all related documents, see [References, page 4-2](#).

Procedure

To deploy a region or site object automatically:

-
- Step 1** In the above reference, refer to Chapter 2, “Configuring Devices with Cisco UGM.”
- Step 2** Read the section Overview of Configuring Managed Devices.
- Step 3** As appropriate, follow the steps in one or more of the following sections (to be accomplished in the following order):
- a. Task 1: Authenticating the Device Object
 - b. Task 2: Selecting a Reload Option After a Configuration Download
 - c. Task 3: Option 1: Building a Configuration File from a Template
 - d. Task 3: Option 2: Using an Existing Configuration File
 - e. Task 3: Option 3: Importing a Configuration File
 - f. (Optional) Task 4: Importing a Configlet
 - g. Task 5: Associating a Configuration File with a Device Object
 - h. (Optional) Task 6: Associating a Configlet with Device Objects
 - i. Task 7: Sending a Configuration File from the Cisco UGM Server to a Device Object’s Startup File

- j. (Optional) Task 8: Sending a Configlet to the Running Configuration File
 - k. (Optional) Task 9: Uploading the Device Startup Configuration File to the Cisco UGM Server
 - l. (Optional) Task 10: Copying the Running Configuration to the Startup Configuration File
 - m. (Optional) Task 11: Viewing and Editing Configuration Files and Configlets
-

Managing Images and Scheduling Actions

Description

Summary	You can use Cisco UGM to manage images and schedule a variety of actions.
Target Platform(s)	Cisco AS5300, Cisco AS5350, Cisco AS5400, Cisco AS5800, Cisco AS5850
Application	See Introduction, page 4-1
Frequency	As needed

Reference

Cisco Universal Gateway Manager Users Guide, Version 2.0

For all related documents, see [References, page 4-2](#).

Procedure

To manage images or schedule actions:

-
- Step 1** In the above reference, refer to Chapter 5, “Managing Images and Schedules with Cisco UGM.”
- Step 2** As appropriate, follow the steps in one or more of the following sections:
- a. Task 1: Authenticating the Device Object
 - b. Task 2: Selecting Upgrade, Reload, and TFTP Host Options
 - c. Task 3: Option 1: Importing a Non-AS5800 Image File into the NAS-File-Repository
 - d. Task 3: Option 2: AS5800 Image File into the NAS-File-Repository
 - e. Task 4: Option 1: Associating Associating an IOS Image with a Device Object
 - f. Task 4: Option 2: Associating a Firmware Image with a Device Object
 - g. Task 4: Option 3: Associating a NAS TFTP Server with a Device
 - h. Task 5: Option 1: Downloading an IOS Image
 - i. Task 5: Option 2: Downloading a Modem Image
 - j. Task 5: Option 3: Downloading an SPE Image
 - k. Task 5: Option 4: Downloading a VFC Image
 - l. (Optional) Task 6: Viewing or Cancelling Scheduled Actions
-

Configuring the Administrative State of Objects

Description

Summary	You can remove an object (T1, E1, E1 combination card, T3, or T3 combination card) from service for maintenance, to minimize the impact on customer traffic. You can then put the object back into service.
Target Platform(s)	Cisco AS5300, Cisco AS5350, Cisco AS5400, Cisco AS5800, Cisco AS5850
Application	See Introduction, page 4-1
Frequency	As needed


Reference

Cisco Universal Gateway Manager Users Guide, Version 2.0

For all related documents, see [References, page 4-2](#).

Procedure

To configure the administrative state of objects:

-
- Step 1** In the above reference, refer to Chapter 4, “Configuring the Administrative State of Objects.”
- Step 2** Read the section Overview of Configuring Administrative States.
-  **Note** Of interest to the Cisco ASAP Solution are the combination cards, although you may still need to support other cards in your network.
-
- Step 3** Read the section Overview of Configuring Administrative States and follow the recommendations therein.
-

Managing Security on Cisco UGM-Managed Devices

Description

Summary	You can set up a variety of levels of administrative access to Cisco UGM-managed devices and their subcomponents. You can specify the following: access specifications (services or features that a user or user group are authorized to run), user groups (defined by a set of users and a set of access specifications), users (with an associated set of access platforms), and access permissions (read only, read write, read-write-admin).
Target Platform(s)	Cisco AS5300, Cisco AS5350, Cisco AS5400, Cisco AS5800, Cisco AS5850
Application	See Introduction, page 4-1
Frequency	As needed

Reference

Cisco Universal Gateway Manager Users Guide, Version 2.0

For all related documents, see [References, page 4-2](#).

Procedure

To manage security on Cisco UGM-managed devices:

-
- Step 1** In the above reference, refer to Chapter 5, “Managing Security on Cisco UGM.”
 - Step 2** Read the section Overview of Managing Security on Cisco UGM.
 - Step 3** Read the section Pres-set Cisco UGM Feature Lists and Access Specifications. The tables in that section list and describe the preset features and access specifications that you can assign to levels of Cisco UGM users. You can modify these and add new ones.
 - Step 4** As appropriate, follow the steps in one or more of the following sections:
 - a. Creating an Access Specification
 - b. Creating a User Group
 - c. Creating Users
 - d. Modifying Users, User Groups, and Access Specifications
-

Managing Device Performance

Description

Summary	You can manage device performance. You can collect selected performance attributes at selected times, store the attributes in a database, poll performance data continuously and store it in a database, view performance data, export performance data to a flat file, check the status of redundant devices, check the status of modems and universal ports, and modify the size of log files.
Target Platform(s)	Cisco AS5300, Cisco AS5350, Cisco AS5400, Cisco AS5800, Cisco AS5850
Application	See Introduction, page 4-1
Frequency	As needed

Reference

Cisco Universal Gateway Manager Users Guide, Version 2.0

For all related documents, see [References, page 4-2](#).

Procedure

To manage device performance:

-
- Step 1** In the above reference, refer to Chapter 8, “Managing the Performance of Cisco UGM-Controlled Devices.”
- Step 2** Read the overview sections in the above chapter.
- Step 3** As appropriate, follow the steps in one or more of the following sections:
- Selecting Performance Polling Intervals
 - Starting and Stopping Performance Polling for the Device and its Subcomponents
 - Viewing SNMP-Polled Performance Data
 - Exporting a File
 - Checking Redundancy ID of Cisco AS5800 and AS5850 Devices
 - Checking the Redundancy Status of a Cisco AS5800 Device
 - Setting Modem-Level Status Polling
 - Setting Controller Logging Levels
 - Modifying the Size of Log Files
-

Managing Faults

Description

Summary	You can identify alarm events and respond accordingly. You can forward specified SNMP traps to a remote host; export alarm events to a text file; and commission and decommission chassis and card objects for maintenance.
Target Platform(s)	Cisco AS5300, Cisco AS5350, Cisco AS5400, Cisco AS5800, Cisco AS5850
Application	See Introduction, page 4-1
Frequency	As needed

Reference

Cisco Universal Gateway Manager Users Guide, Version 2.0

For all related documents, see [References, page 4-2](#).

Procedure

To monitor events:

-
- Step 1** In the above reference, refer to Chapter 7, “Managing Faults with Cisco UGM.”
- Step 2** Read the overview sections in the above chapter.
- Step 3** As appropriate, follow the steps in one or more of the following sections:
- a. Clearing Alarm Events
 - b. Using the Event Browser
 - c. Using the Query Editor
 - d. Specifying New Trap Forwarding Hosts
 - e. Specifying New Trap Specifiers for a Trap Forwarding Host
 - f. Changing Previously Specified Trap Forwarding Data
 - g. Removing Previously Specified Trap Forwarding Data
 - h. Exporting Alarm Events to a File
-

Managing Presence Polling and Loss of Communication

Description

Summary	To detect loss of communication with devices and cards, Cisco UGM uses presence polling. There are a variety of options for managing polling and communications. You can also commission or decommission a device or card.
Target Platform(s)	Cisco AS5300, Cisco AS5350, Cisco AS5400, Cisco AS5800, Cisco AS5850
Application	See Introduction, page 4-1
Frequency	As needed

Reference

Cisco Universal Gateway Manager Users Guide, Version 2.0

For all related documents, see [References, page 4-2](#).

Procedure

To manage presence polling and communication with devices:

-
- | | |
|---------------|---|
| Step 1 | In the above reference, refer to Chapter 8, “Presence Polling and Loss of Communication.” |
| Step 2 | Read the overview sections in the above chapter. |
| Step 3 | As appropriate, follow the steps in one or more of the following sections: <ol style="list-style-type: none">Setting Presence Polling Intervals for Devices in Normal, Errored, and Reload StatesSetting the Presence Polling Interval for CardsSetting the Number of Retries Before Loss of CommunicationCommissioning and Decommissioning a Device or Card |
-



Managing SS7 Signaling Components: Using Cisco MGC Node Manager

Introduction

This chapter presents operations and maintenance tasks related to the Cisco ASAP Solution and the PSTN gateway solutions that are provided from the application Cisco Media Gateway Controller Node Manager (Cisco MNM). Cisco MNM is a comprehensive element management system that operates and maintains the Cisco SC2200 (also known as the Cisco PGW 2200), as well as related network components, by integrating management interfaces and functionality into a single interface and data repository. With this application you can manage security; deploy a site, object, or network; use polling to monitor network performance; manage traps and events; and view information about network devices. The tasks in this chapter are listed below.



Note

The Cisco PGW 2200 configured for signaling is also referred to in a variety of documents as the Cisco SC2200, the earlier term. The term “Cisco SC2200” is applicable to the Cisco ASAP Solution and Release 1.3 of the Cisco SS7 Interconnect for Voice Gateways Solution, and the term “Cisco PGW 2200” is applicable to the Cisco PSTN Gateway Solution and Release 2.0 of the Cisco SS7 Interconnect for Voice Gateways Solution.

This chapter presents the following major management topics:

- [Configuring Devices for Management](#)
- [Managing Security](#)
- [Deploying a Site, Object, or Network](#)
- [Monitoring Network Performance](#)
- [Managing Traps and Events](#)
- [Viewing Information about Network Devices](#)
- [Event Messages and Problem Correction](#)



Tip

See also [Task Summary, page 5-2](#).

Target Platforms

The Cisco MGC Node Manager manages the following components of the Cisco ASAP Solution and the PSTN gateway solutions: Cisco MGC (Cisco SC2200/Cisco PGW 2200), Cisco SLT (Cisco 2611 or 2651), Cisco Catalyst 5500 switch, and Cisco BAMS.

References

Cisco MGC Release 7 (for the Cisco ASAP Solution and Release 1.3 of the Cisco SS7 Interconnect for Voice Gateways Solution) and Cisco MGC Release 9 (for Cisco PSTN Gateway Solution and Release 2.0 of the Cisco SS7 Interconnect for Voice Gateways Solution) require different versions of Cisco MNM. This chapter refers to procedures in Cisco MNM Release 1.5 *only*.

Cisco MGC Release 7

For the following procedures, refer to *Cisco Media Gateway Controller Node Manager User's Guide 1.5* at the following URL:

<http://www.cisco.com/univercd/cc/td/doc/product/access/sc/rel8/cmmngr/>

**Note**

Cisco MNM is built on the Cisco Element Management Framework (CEMF), a carrier-class network management framework. To understand this framework, refer to the section Overview of CEMF in the above document.

Cisco MGC Release 9

For documentation or Cisco MNM Release 2.1, refer to *Cisco Media Gateway Controller Node Manager User's Guide, Version 2.1* at the following URL:

<http://www.cisco.com/univercd/cc/td/doc/product/access/sc/rel9/cmm21/index.htm>

Task Summary

The tasks in this chapter are listed below, grouped by major category.

Configuring Devices for Management

- [Configuring Network Devices for Management](#)

Managing Security

- [Setting Up Cisco MNM Security](#)

Deploying a Site, Object, or Network

- [Deployment: Using a Seed File to Deploy a Cisco MGC Network](#)
- [Deployment: Manually Deploying a Site, Object, or Network](#)

- [Discovery: Discovering a Cisco SLT, LAN Switch, Cisco MGC Host, or BAMS](#)
- [Managing Software Images and Configurations](#)

Monitoring Network Performance

- [Monitoring Network Performance: Setting Polling Parameters](#)
- [Monitoring Network Performance: Viewing and Managing Performance Data](#)

Managing Traps and Events

- [Managing Traps and Events: Managing, Clearing, and Forwarding Traps](#)
- [Managing Traps and Events: Managing Events](#)
- [Managing Traps and Events: Miscellaneous Tasks](#)
- [Managing Traps and Events: Setting How Long Alarms are Stored](#)

Viewing Information about Network Devices

- [Viewing Information about Network Devices: Available Information](#)
- [Viewing Information about Network Devices: Using Diagnostic Tools](#)

Event Messages and Problem Correction

- [Event Messages: BAMS, Cisco MGC, and Cisco MNM](#)

Configuring Network Devices for Management

Description

Summary	You must configure a variety of SNMP parameters (SNMP community strings, SNMP trap destinations, other miscellaneous SNMP settings) on a device before Cisco MNM can manage it.
Target Platform(s)	Cisco MGC (Cisco SC2200), Cisco SLT (Cisco 2611), Cisco Catalyst 5500 switch (see Note below), Cisco BAMS
Application	See Introduction, page 5-1
Frequency	As needed


Note

The only LAN switch supported by Cisco MNM is the Cisco Catalyst 5500.

Reference

Cisco Media Gateway Controller Node Manager User Guide 1.5

For all related documentation, see [References, page 5-2](#).

Procedure

To create, modify, or delete a UG group:

-
- Step 1** In the above reference, refer to Chapter 3, “Configuring Network Devices for Management.”
 - Step 2** Read the section Introduction to Device Configuration.
 - Step 3** As appropriate, follow the steps in one or more of the following sections:
 - a. Configuring the Cisco MGC
 - b. Configuring a Cisco SLT (Cisco 2611)
 - c. Configuring the LAN Switch (Catalyst 5500)
 - d. Configuring Cisco BAMS
-

Setting Up Cisco MNM Security

Description

Summary	Cisco MNM allows system administrators to control user access and user privileges. User accounts can be collected into user groups, and lists of accessible features can be established for a user. Tasks include setting up new accounts, creating new access specifications, creating typical types of users, modifying users, modifying user groups, modifying access specifications, and changing the administrative password.
Target Platform(s)	Cisco MGC (Cisco SC2200), Cisco SLT (Cisco 2611), Cisco Catalyst 5500 switch, Cisco BAMS
Application	See Introduction, page 5-1
Frequency	As needed

Reference

Cisco Media Gateway Controller Node Manager User Guide 1.5

For all related documentation, see [References, page 5-2](#).

Procedure

To set up Cisco MNM security:

-
- Step 1** In the above reference, refer to Chapter 5, “Setting Up CMNM Security.”
 - Step 2** Read the section Introduction to Cisco MNM Security. That section lists and describes ready-made feature lists.
 - Step 3** As appropriate, follow the steps in one or more of the following sections:
 - a. Setting Up New Accounts
 - b. Creating User Groups
 - c. Creating New Access Specifications
 - d. Creating Typical Types of Users
 - e. Modifying Users
 - f. Modifying User Groups
 - g. Modifying Access Specifications
 - h. Changing the Administrative Password
-

Deployment: Using a Seed File to Deploy a Cisco MGC Network

Description

Summary	Deployment is the addition of objects (sites, objects, or networks) to the CEMF network model. Cisco MNM allows you to deploy Cisco MGC nodes and subobjects either in bulk, through the use of a seed file, or manually. This task relates to the use of a seed file to deploy a Cisco MGC network.
Target Platform(s)	Cisco MGC (Cisco SC2200), Cisco SLT (Cisco 2611), Cisco Catalyst 5500 switch, Cisco BAMS
Application	See Introduction, page 5-1
Frequency	As needed

Reference

Cisco Media Gateway Controller Node Manager User Guide 1.5

For all related documentation, see [References, page 5-2](#).

Procedure

To use a seed file to deploy a Cisco MGC network:

-
- | | |
|---------------|---|
| Step 1 | In the above reference, refer to Chapter 6, “Deploying a Site, Object, or Network.” |
| Step 2 | Read the sections Introduction to Deployment and Deploying a Network Using a Seed File. |
| Step 3 | Read the section Specifying a Deployment Seed File and follow the steps therein. |
-

Notes

- *Related tasks:* [Deployment: Manually Deploying a Site, Object, or Network, page 5-7](#)

Deployment: Manually Deploying a Site, Object, or Network

Description

Summary	Deployment is the addition of objects (sites, objects, or networks) to the CEMF network model. Cisco MNM allows you to deploy Cisco MGC nodes and subobjects either in bulk, through the use of a seed file, or manually. This task relates to the manual deployment of a Cisco MGC network.
Target Platform(s)	Cisco MGC (Cisco SC2200), Cisco SLT (Cisco 2611), Cisco Catalyst 5500 switch, Cisco BAMS
Application	See Introduction, page 5-1
Frequency	As needed

Reference

Cisco Media Gateway Controller Node Manager User Guide 1.5

For all related documentation, see [References, page 5-2](#).

Procedure

To deploy a site, object, or network manually:

-
- Step 1** In the above reference, refer to Chapter 6, “Deploying a Site, Object, or Network.”
 - Step 2** Read the sections Introduction to Deployment and Manually Deploying a Site, Object, or Network.
 - Step 3** Open the deployment wizard. Refer to the section Opening the Deployment Wizard.
 - Step 4** As appropriate, follow the steps in one or more of the following sections:
 - a. Deploying a Cisco MGC Node
 - b. Deploying a Cisco MGC Host
 - c. Deploying a Cisco SLT
 - d. Deploying a LAN Switch
 - e. Deploying a Billing and Measurements Server (Cisco BAMS)
-

Notes

- *Related tasks:* [Deployment: Using a Seed File to Deploy a Cisco MGC Network, page 5-6](#)

Discovery: Discovering a Cisco SLT, LAN Switch, Cisco MGC Host, or BAMS

Description

Summary	When a Cisco SLT, LAN switch, Cisco MGC host, or BAMS is deployed, its subrack components are queried and deployed. Cisco MNM can discover the subrack components, and their relationships, of these devices.
Target Platform(s)	Cisco MGC (Cisco SC2200), Cisco SLT (Cisco 2611), Cisco Catalyst 5500 switch, Cisco BAMS
Application	See Introduction, page 5-1
Frequency	As needed

Reference

Cisco Media Gateway Controller Node Manager User Guide 1.5

For all related documentation, see [References, page 5-2](#).

Procedure

To discover a Cisco SLT, LAN switch, Cisco MGC host, or BAMS:

-
- Step 1** In the above reference, refer to Chapter 6, “Deploying a Site, Object, or Network.”
- Step 2** Read the section Subrack Discovery. Discovery varies according to the type of device or object.
- Step 3** As appropriate, read the following sections for the type of discovery desired:
- To discover a Cisco MGC host, BAMS, or unknown/unsupported device, read Cisco MGC Host and BAMS Discovery.
 - To discover a Cisco SLT, as well as TDM (DS1) interfaces and SS7 channels, read Cisco SLT Discovery.
 - To discover slots, VLANs, and ports on a Cisco Catalyst 5500 series LAN switch, read Catalyst 5500 Discovery.
 - To discover a Cisco MGC node, including trunking, signaling, and dial plan components, read Cisco MGC Node Discovery.
-

Managing Software Images and Configurations

Description

Summary	Cisco MNM lets you manage software images and configuration files on Cisco MGC nodes. Tasks include backing up (uploading) and restoring (downloading) configurations of the Cisco MGC host, BAMS, Cisco SLT, and LAN switch; downloading software modules and patches to Cisco MGC nodes; backing up software images from a Cisco SLT or LAN switch; and automating or scheduling configuration backups.
Target Platform(s)	Cisco MGC (Cisco SC2200), Cisco SLT (Cisco 2611), Cisco Catalyst 5500 switch, Cisco BAMS
Application	See Introduction, page 5-1
Frequency	As needed

Reference

Cisco Media Gateway Controller Node Manager User Guide 1.5

For all related documentation, see [References, page 5-2](#).

Procedure

To upload or download an image or configuration file for a Cisco SLT, LAN switch, Cisco MGC host, or BAMS:

-
- Step 1** In the above reference, refer to Chapter 6, “Deploying a Site, Object, or Network.”
 - Step 2** Read the section Managing Software Images and Configurations.
 - Step 3** As appropriate, follow the steps in one or more of the following sections:
 - a. Uploading and Downloading Cisco SLT and LAN Switch Images and Configurations
 - b. Uploading and Downloading Cisco MGC Host and BAMS Images and Configurations
-

Monitoring Network Performance: Setting Polling Parameters

Description

Summary	Cisco MNM lets you monitor performance statistics gathered from network elements. Tasks include setting polling frequencies; starting and stopping polling; decommissioning, rediscovering, and rebooting devices; viewing (graphing) performance data; viewing raw data; viewing charts; viewing logs; exporting performance data; and printing performance files. These tasks relate to viewing and managing performance data.
Target Platform(s)	Cisco MGC (Cisco SC2200), Cisco SLT (Cisco 2611), Cisco Catalyst 5500 switch, Cisco BAMS
Application	See Introduction, page 5-1
Frequency	As needed

Reference

Cisco Media Gateway Controller Node Manager User Guide 1.5

For all related documentation, see [References, page 5-2](#).

Procedure

To view, archive, export, and print performance data:

-
- Step 1** In the above reference, refer to Chapter 7, “Using Polling to Monitor Network Performance.”
- Step 2** Read the section Viewing Performance Data and follow the steps therein to set a variety of parameters and view the data of interest.
- Step 3** As appropriate, follow the steps in one or more of the following sections:
- Viewing Raw Data
 - Viewing a Chart
 - Viewing a Performance Log
 - Setting How Performance Data is Archived
 - Exporting Performance Data
 - Printing a Performance File
-

Notes

- *Related tasks:* [Monitoring Network Performance: Viewing and Managing Performance Data](#), page 5-13

Monitoring Network Performance: Viewing and Managing Performance Data

Description

Summary	<p>Cisco MNM lets you monitor performance statistics gathered from network elements. Tasks include setting polling frequencies; starting and stopping polling; decommissioning, rediscovering, and rebooting devices; viewing (graphing) performance data; viewing raw data; viewing charts; viewing logs; exporting performance data; and printing performance files.</p> <p>These tasks relate to setting polling frequencies and start and stop times, as well as decommissioning, rediscovering, and rebooting device. Decommissioning a device prevents it from being presence polled or performance polled. Commissioning it reinstates presence polling.</p>
Target Platform(s)	Cisco MGC (Cisco SC2200), Cisco SLT (Cisco 2611), Cisco Catalyst 5500 switch, Cisco BAMS
Application	See Introduction, page 5-1
Frequency	As needed

Reference

Cisco Media Gateway Controller Node Manager User Guide 1.5

For all related documentation, see [References, page 5-2](#).

Procedure

To set polling parameters and determine which devices are to be polled:

-
- Step 1** In the above reference, refer to Chapter 7, “Using Polling to Monitor Network Performance.”
 - Step 2** Read the sections Introduction to Performance Monitoring and How Performance Data is Collected. Note the performance counters and their descriptions for the various components and network interfaces
 - Step 3** Read the section Cisco MGC Host Configuration Performance Counters. There are a number of files on the Cisco MGC host that select performance counters and determine their frequency of collection. There are also measurement filters you can apply.
 - Step 4** Open the Performance Manager. Refer to the section Opening the Performance Manager and follow the steps therein.
 - Step 5** Read the section Setting Polling Frequencies.
 - Step 6** As appropriate, follow the steps in one or more of the following sections:
 - a. Changing Collection Defaults

- b. Setting Different Polling Frequencies
 - c. Decommissioning, Rediscovering, and Rebooting Devices
 - d. Starting Polling on a Device
-

Notes

- *Related tasks:* [Monitoring Network Performance: Setting Polling Parameters, page 5-11](#)

Managing Traps and Events: Managing, Clearing, and Forwarding Traps

Description

Summary	Critical to network management is the ability to identify specific undesirable system events (faults) and resolve them as soon as possible. Traps are connectivity-related messages about various events that are generated by an element. Traps are converted to alarms, which are displayed in the Cisco MNM Event Browser. An event is a notification from a managed entity that a certain condition has just occurred. Usually events represent error conditions on managed elements. These tasks relate to managing, clearing, and forwarding connectivity traps for Cisco MGC components.
Target Platform(s)	Cisco MGC (Cisco SC2200), Cisco SLT (Cisco 2611), Cisco Catalyst 5500 switch, Cisco BAMS
Application	See Introduction, page 5-1
Frequency	As needed

Reference

[Cisco Media Gateway Controller Node Manager User Guide 1.5](#)

For all related documentation, see [References, page 5-2](#).

Procedure

To manage, clear, and forward traps and events on Cisco MGC components:

Step 1 In the above reference, refer to Chapter 8, “Managing Traps and Events.”



Note As appropriate, apply the information presented in any or all of the following sections.

- Step 2** Read the sections Introduction to Fault Management, How CEMF Models Events, How Cisco MNM Manages Faults, and Presence/Status Polling.
- Step 3** To *manage traps*, read the section How Traps are Managed for Network Devices. Note the alarms/traps definitions and explanations, as well as related MIBs, for the following components: Cisco SLT, Cisco Catalyst LAN switch, and Cisco MGC host.
- Step 4** To *clear traps*, read the section How Traps Are Cleared Using Correlation Files. CEMF Clear Correlation files are used to clear traps for a Cisco MGC host, a Cisco SLT, and a Cisco Catalyst LAN switch.

- Step 5** To *forward traps* (to northbound management systems), read the section Forwarding Traps to Other Systems and follow the steps therein. See *Special issues*, below.
-

Notes

- *Special issues*: Cisco MNM forwards only SNMP Version 1 traps to northbound systems.
- *Related tasks*: [Managing Traps and Events: Managing Events, page 5-17](#)

Managing Traps and Events: Managing Events

Description

Summary	Critical to network management is the ability to identify specific undesirable system events (faults) and resolve them as soon as possible. Traps are connectivity-related messages about various events that are generated by an element. Traps are converted to alarms, which are displayed in the Cisco MNM Event Browser. An event is a notification from a managed entity that a certain condition has just occurred. Usually events represent error conditions on managed elements. These tasks relate to managing events.
Target Platform(s)	Cisco MGC (Cisco SC2200), Cisco SLT (Cisco 2611), Cisco Catalyst 5500 switch, Cisco BAMS
Application	See Introduction, page 5-1
Frequency	As needed


Reference

Cisco Media Gateway Controller Node Manager User Guide 1.5

For all related documentation, see [References, page 5-2](#).

Procedure

To manage, clear, and forward traps and events on Cisco MGC components:

-
- Step 1** In the above reference, refer to Chapter 8, “Managing Traps and Events.”
-
-  **Note** As appropriate, apply the information presented in any or all of the following sections.
-
- Step 2** Read the sections Introduction to Fault Management, How CEMF Models Events, How Cisco MNM Manages Faults, and Presence/Status Polling.
- Step 3** To *use the Event Browser*, read the sections Opening the Event Browser and Overview of the Event Browser Screen.
- Step 4** To *filter events*, read the section Filtering Events Using Queries. As appropriate, follow the steps in one or both of the following subsections:
- a. Setting Filter Criteria
 - b. Modifying Filter Criteria

- Step 5** To *sort events*, read the section *Sorting Events* and select the sorting options as appropriate.
- Step 6** To *manage events*, read the section *Managing Events*. As appropriate, follow the steps in one or both of the following subsections:
- a. Managing an Event from the Window
 - b. Managing an Event from the Menu Bar
- Step 7** To view incoming events that are *automatically updated* in the Event Browser window, read the section *Enabling Auto or Manual Update* and select the auto option as appropriate. Deselect the option to revert to manual update mode.
- Step 8** To *color code events*, read the section *Setting How Events Are Color-Coded* and select the appropriate option.
- Step 9** To view event history, read the section *Viewing the Event History* and follow the steps therein. Note also the following related tasks:
- a. Refreshing the Event Window
 - b. Viewing a Full Description of an Event
-

Notes

- *Related tasks:* [Managing Traps and Events: Managing, Clearing, and Forwarding Traps, page 5-15](#), [Managing Traps and Events: Miscellaneous Tasks, page 5-19](#), [Managing Traps and Events: Setting How Long Alarms are Stored, page 5-21](#)

Managing Traps and Events: Miscellaneous Tasks

Description

Summary	Critical to network management is the ability to identify specific undesirable system events (faults) and resolve them as soon as possible. Traps are connectivity-related messages about various events that are generated by an element. Traps are converted to alarms, which are displayed in the Cisco MNM Event Browser. An event is a notification from a managed entity that a certain condition has just occurred. Usually events represent error conditions on managed elements. You can manage Cisco MGC host faults and performance from the MGC Toolbar. These tasks relate to using the Cisco MGC toolbar to view alarms, measurements, CDRs, log files, and trace files, as well as to perform other management activities.
Target Platform(s)	Cisco MGC (Cisco SC2200), Cisco SLT (Cisco 2611), Cisco Catalyst 5500 switch, Cisco BAMS
Application	See Introduction, page 5-1
Frequency	As needed

Reference

Cisco Media Gateway Controller Node Manager User Guide 1.5

For all related documentation, see [References, page 5-2](#).

Procedure

To use the Cisco MGC toolbar for miscellaneous management tasks:

Step 1 In the above reference, refer to Chapter 8, “Managing Traps and Events.”



Note As appropriate, apply the information presented in any or all of the following sections.

Step 2 Read the section Using the Cisco MGC Tool Bar. As appropriate, follow the steps in one or more of the following sections.

- a. To *view or search alarms and measurements*, read the section Alarm and Measurements View and follow the steps therein.
- b. To *view or search call data records (CDRs)*, read the section CDR Viewer and follow the steps therein.

- c. To view the contents of the configuration library, read the section CONFIG-LIB Viewer and follow the steps therein.
 - d. To view or search a log file, read the section Log Viewer and follow the steps therein.
 - e. To view a trace file, read the section Trace Viewer and follow the steps therein.
 - f. To verify a translation, read the section Translation Verification and follow the steps therein.
 - g. To manage the files associated with the Cisco MGC tool bar, read the section File Options and follow the steps therein.
-

Notes

- *Related tasks:* [Managing Traps and Events: Managing, Clearing, and Forwarding Traps, page 5-15](#), [Managing Traps and Events: Managing Events, page 5-17](#), [Managing Traps and Events: Setting How Long Alarms are Stored, page 5-21](#)

Managing Traps and Events: Setting How Long Alarms are Stored

Description

Summary	<p>Critical to network management is the ability to identify specific undesirable system events (faults) and resolve them as soon as possible. Traps are connectivity-related messages about various events that are generated by an element. Traps are converted to alarms, which are displayed in the Cisco MNM Event Browser. An event is a notification from a managed entity that a certain condition has just occurred. Usually events represent error conditions on managed elements.</p> <p>All alarms are automatically stored in the CEMF database. CEMF does not archive old alarms, but it can be configured to delete alarms of a specific age and state.</p>
Target Platform(s)	Cisco MGC (Cisco SC2200), Cisco SLT (Cisco 2611), Cisco Catalyst 5500 switch, Cisco BAMS
Application	See Introduction, page 5-1
Frequency	As needed

Reference

Cisco Media Gateway Controller Node Manager User Guide 1.5

For all related documentation, see [References, page 5-2](#).

Procedure

To set how long alarms are stored:

-
- | | |
|---------------|---|
| Step 1 | In the above reference, refer to Chapter 8, “Managing Traps and Events.” |
| Step 2 | Read the section Setting How Long Alarms Are Stored and follow the steps therein. |
-

Notes

- *Related tasks:* [Managing Traps and Events: Managing, Clearing, and Forwarding Traps, page 5-15](#), [Managing Traps and Events: Managing Events, page 5-17](#), [Managing Traps and Events: Miscellaneous Tasks, page 5-19](#)

Viewing Information about Network Devices: Available Information

Description

Summary	You can use Cisco MNM to view a considerable amount of information related to Cisco MGC components: Cisco MGC host accounts, properties, and file systems; Cisco SLT accounts and properties; LAN switch accounts and properties; BAMS accounts, properties, and file systems; CIAgent device information; and Ethernet, TDM, and serial interface properties.
Target Platform(s)	Cisco MGC (Cisco SC2200), Cisco SLT (Cisco 2611), Cisco Catalyst 5500 switch, Cisco BAMS
Application	See Introduction, page 5-1
Frequency	As needed

Reference

Cisco Media Gateway Controller Node Manager User Guide 1.5

For all related documentation, see [References, page 5-2](#).

Procedure

To view available information about network devices:

-
- Step 1** In the above reference, refer to Chapter 9, “Viewing Information About Network Devices.”
- Step 2** Read the sections Introduction and Viewing Accounts and Properties. As appropriate, read the following sections and follow the steps therein:
- a. Viewing Cisco MGC Host Accounts
 - b. Viewing Cisco MGC Host Properties
 - c. Viewing Cisco MGC Host File Systems
 - d. Viewing Cisco SLT Accounts
 - e. Viewing Cisco SLT Properties
 - f. Viewing LAN Switch Accounts
 - g. Viewing LAN Switch Properties
 - h. Viewing BAMS Accounts
 - i. Viewing BAMS Properties
 - j. Viewing BAMS File Systems

- k. Viewing CIAgent Device Information
 - l. Viewing Ethernet Interface Properties
 - m. Viewing TDM Interface Properties
 - n. Viewing Serial Interface Properties
-

Notes

- *Related tasks:* [Viewing Information about Network Devices: Using Diagnostic Tools, page 5-24](#)

Viewing Information about Network Devices: Using Diagnostic Tools

Description

Summary	Cisco MNM provides a number of tools to monitor the health of network elements. These include ping and traceroute, as well as diagnostic and configuration tools that depend on the type of device being tested. Cisco MNM also provides an entire suite of tools for testing the operating status of the MGC host. Other diagnostic tasks include initiating a configuration audit, retrieving alarm logs, and monitoring file systems on devices where the supported SNMP agent is installed.
Target Platform(s)	Cisco MGC (Cisco SC2200), Cisco SLT (Cisco 2611), Cisco Catalyst 5500 switch, Cisco BAMS
Application	See Introduction, page 5-1
Frequency	As needed

Reference

Cisco Media Gateway Controller Node Manager User Guide 1.5

For all related documentation, see [References, page 5-2](#).

Procedure

To use diagnostic tools, initiate a configuration audit, retrieve alarm logs, or monitor file systems:

-
- Step 1** In the above reference, refer to Chapter 9, “Viewing Information About Network Devices.”
 - Step 2** To use a variety of diagnostic and configuration tools, read the section Using Diagnostic Tools and select the tools appropriate to the device in question.
 - Step 3** To view the status of the MGC host, read the section MGC Host Status Check and select from among the operation commands.
 - Step 4** To initiate a configuration audit (which compares the trunking information on the BAMS to that on associated Cisco MGC hosts), read the section Configuration Audit and use the MML command therein.
 - Step 5** To retrieve alarms and process status, read the section Processes and Alarms and use the MML commands therein.
 - Step 6** To monitor file systems on devices where the supported SNMP agent is installed, read the section File System Monitor and follow the instructions therein.

Notes

- *Related tasks:* [Viewing Information about Network Devices: Available Information](#), page 5-22

Event Messages: BAMS, Cisco MGC, and Cisco MNM

Description

Summary	The Cisco MNM Event Browser can display event messages related to the BAMS, the Cisco MGC, and Cisco MNM internal messages. With respect to BAMS and Cisco MGC, it provides references to relevant documentation. With respect to Cisco MNM internal even messages, it provides a short explanation of the message and recommended actions. Tasks include solving deployment and discovery errors once they are found.
Target Platform(s)	BAMS host, Cisco MGC (Cisco SC2200), Cisco MNM host
Application	See Introduction, page 5-1
Frequency	As needed

Reference

Cisco Media Gateway Controller Node Manager User Guide 1.5

For all related documentation, see [References, page 5-2](#).

Procedure

To view BAMS, Cisco MGC, or Cisco MNM internal event messages, as well as solve deployment or discovery errors:

-
- Step 1** In the above reference, refer to Appendix A, “BAMS, Cisco MGC, and Cisco MNM Messages.”
 - Step 2** To view *BAMS or Cisco MGC host messages*, read the section Looking Up BAMS and Cisco MGC Messages and follow the steps therein.
 - Step 3** To interpret *Cisco MGC host messages*, read the section Cisco MGC Host Messages and follow the instructions therein.
 - Step 4** To interpret *BAMS messages*, read the section BAMS Messages and follow the instructions therein.
 - Step 5** To interpret *Cisco MNM internal event messages* and take corrective action, read Cisco MNM Internal Messages and note the table therein.

- Step 6** To *solve deployment and discovery errors*, read the section Solving Deployment and Discovery Errors. As appropriate, follow the steps in one or more of the following sections:
- a. Changing Password or Community Strings
 - b. Changing IP Address
 - c. Rediscovering a Device After a Problem
-



Operating and Maintaining Cisco Devices: Using Cisco Info Center

Introduction

This chapter presents operations and maintenance tasks for the Cisco Info Center (CIC) that are relevant to the Cisco ASAP Solution and Cisco SS7 Interconnect Solution.

CIC is a service-level alarm monitoring and diagnostics tool that provides network fault and performance management. Depending on which Info Mediators you have purchased licenses for and installed, you can use CIC to monitor the following types of events from the Cisco hardware and software that support the Cisco ASAP Solution and Cisco SS7 Interconnect Solution:

- Cisco Element Management Framework (CEMF) Events, which includes the following:
 - Cisco Media Gateway Node Manager (Cisco MNM) events
 - Cisco Universal Gateway Manager (UGM) events
 - Universal Gateway events
- Cisco 3660 Multiservice Platform Router events
- Cisco SLT (Cisco 2611) events
- Cisco PGW2200/SC2200 events
- Generic SNMP alarms from Windows or Sun servers

This chapter presents the following major operations and maintenance tasks:

- [Installing and Configuring Relevant Components of CIC](#)
- [Operating and Maintaining CIC Components](#)
- [Managing Events and Traps Using CIC](#)



Tip

See also [Task Summary, page 6-2](#).

Target Platforms

The Cisco Info Center application manages the following components of the Cisco ASAP Solution and Cisco SS7 Interconnect Solution:

- Cisco 3660 series
- Cisco AS5000 series

References

For information about how to install, upgrade, and configure CIC, refer to *Cisco Info Center Installation and Configuration* at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/info_ctr/3_0/install/index.htm

The topics relevant to the Cisco ASAP Solution and PSTN gateway solutions include the following:

- Overview of Cisco Info Center
- Overview of Installation and Configuration
- Installing and Configuring the Multi-System Architecture
- Installing and Configuring the Single-System Architecture
- Upgrading to Cisco Info Center 3.0
- Installation Utilities

For information about how to use CIC, refer to *Cisco Info Center User Guide* at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/info_ctr/3_0/user_gd/index.htm

For information about how the Cisco Info Center works, refer to *Cisco Info Center Administrator Reference* at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/info_ctr/3_0/admin/index.htm

For information about how to use and operate the Info Mediators in the Cisco Info Center, refer to *Cisco Info Center Mediator and Gateway Reference* at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/info_ctr/3_0/medgw/index.htm

Task Summary

The tasks in this chapter are listed below, grouped by major category.

Installing and Configuring Relevant Components of CIC

The following are the CIC components that are applicable to the Cisco ASAP Solution and Cisco PSTN Gateway Solution. For information about how to install and configure these components, refer to the *Cisco Info Center Installation and Configuration*.

- Cisco Info Server
- Info Mediators
- Syslog Trap Generator

- [Process Control System](#)
- [Cisco Info Admin Desktop](#)

Operating and Maintaining CIC Components

- [Modifying Configurations Using the Configuration Manager](#)
- [Configuring Remote Processes Using Process Control](#)
- [Manually Starting and Stopping CIC Components](#)
- [Starting and Stopping the Cisco Info Server](#)
- [Creating a New Cisco Info Server](#)
- [Managing the Cisco Info Server Using CLI Options](#)
- [Creating and Editing the Interfaces File](#)

Managing Events and Traps Using CIC

- [Creating, Editing, and Managing Filters Using the Filter Builder](#)
- [Using the Event List to Display Alerts](#)
- [Creating, Editing, and Managing Views Using View Builder](#)
- [Managing Objects Using the Objective View](#)
- [Managing User Access](#)

Troubleshooting

- [Troubleshooting: Using CIC Diagnostic Tools](#)

Manually Starting and Stopping CIC Components

Description

Summary	The CIC components can be manually started and stopped.
Target Platform(s)	Cisco AS5000 series, Cisco 3660
Application	CEMF, CIC
Frequency	As needed

Reference

Cisco Info Center Installation and Configuration

For all related documentation, see [References](#), page 6-2.

Procedure

To start and stop the CIC components manually:

-
- | | |
|---------------|--|
| Step 1 | To start the installed Cisco Info Center components manually, execute the following command:
<code>host# /opt/Omnibus/bin/nco_pa_start</code> |
| Step 2 | To shut down the running Cisco Info Center components manually, execute the following command:
<code>host# opt/Omnibus/bin/nco_pa_shutdown</code> |
-

Starting and Stopping the Cisco Info Server

Description

Summary	Cisco Info Center comes with a set of network event views that allow you to monitor a variety of Cisco hardware and software. The Cisco Info Server is the core of Cisco Info Center and is where all event and status data is stored and managed.
Target Platform(s)	Cisco AS5000 series, Cisco 3660
Application	CEMF, CIC
Frequency	As needed

Reference

Cisco Info Center Administrator Reference

For all related documentation, see [References](#), page 6-2.

Procedure

To start or stop the Cisco Info Server:

-
- Step 1** In the above reference, refer to Chapter 1, “Cisco Info Server.”
 - Step 2** Read the sections Introduction to the Cisco Info Server, Starting and Stopping the Info Server, and Multiple Cisco Info Servers.
 - Step 3** As appropriate, follow the steps in one or more of the following:
 - a. Starting the Info Server
 - b. Stopping the Info Server
 - c. Starting and Stopping an Info Server From a Remote Machine
-

Modifying Configurations Using the Configuration Manager

Description

Summary	<p>The Configuration Manager allows the administrator to define graphically how the Cisco Info Center system should be configured. It then updates the Cisco Info Server, distributing the information to Cisco Info Center nodes. The tabs on the Configuration Manager window allow you to select the following areas of configuration:</p> <ul style="list-style-type: none"> • Automations—Define event conditions that trigger automatic responses by the system. • Users—Manage user access to Cisco Info Center. • Properties—Edit the settings in the properties file for the current Info Server. • Menus—Configure how system menus appear to end users. • Classes—Define event classes. • Conversions—Specify data conversion for data fields in events. • Column Visuals—Specify how the information in event fields appears on the event list display and in other tools.
Target Platform(s)	Cisco AS5000 series, Cisco 3660
Application	CEMF, CIC
Frequency	As needed

Reference

Cisco Info Center Administrator Reference

For all related documentation, see [References, page 6-2](#).

Procedure

To use the Configuration Manager for making changes to the CIC configuration:

-
- Step 1** In the above reference, refer to Chapter 3, “Using the Configuration Manager.”
- Step 2** Read the sections Starting the Configuration Manager, Conversions, Column Visuals, and Classes.
- Step 3** As appropriate, follow the steps in one or more of the following:
- Creating, editing, deleting conversions, column visuals, and classes.
-

Configuring Remote Processes Using Process Control

Description

Summary	<p>The Cisco Info Center Process Control system allows you to configure and manage UNIX processes remotely. The system is designed to simplify the configuration and management of Cisco Info Center components such as Cisco Info Server and Info Mediators.</p> <p>The Process Control system provides centralized operations management consisting of the following elements:</p> <ul style="list-style-type: none">• Master Process Control Server, from where the complete Cisco Info Center configuration can be managed• Process Control Agents, which are programs installed on each host with the responsibility of managing processes.
Target Platform(s)	Cisco AS5000 series, Cisco 3660
Application	CEMF, CIC
Frequency	As needed

Reference

[Cisco Info Center Administrator Reference](#)

For all related documentation, see [References](#), page 6-2.

Procedure

To configure and manage UNIX processes remotely:

-
- | | |
|---------------|---|
| Step 1 | In the above reference, refer to Chapter 2, “Process Control.” |
| Step 2 | Read the sections Process Control System Configuration, Process Control Service and Process Configuration, Process Control Management, Process Control Agent Daemon Command Line Options. |
| Step 3 | As appropriate, follow the steps in one or more of the above sections. |
-

Creating a New Cisco Info Server

Description

Summary	Any number of Info Servers can be created on a single machine.
Target Platform(s)	Cisco AS5000 series, Cisco 3660
Application	CEMF, CIC
Frequency	As needed

Reference

Cisco Info Center Administrator Reference

For all related documentation, see [References, page 6-2](#).

Procedure

To create single or multiple Cisco Info Center Servers:

-
- Step 1** In the above reference, refer to Chapter 1, “Cisco Info Server.”
- Step 2** Read the section Multiple Cisco Info Servers and follow the steps in the following:
- a. Creating a New Cisco Info Server
 - b. Service File Entries for Multiple Cisco Info Servers
-

Using the Event List to Display Alerts

Description

Summary	<p>The Event List displays alerts such as an event, alarm, message, or data that the Cisco Info Server receives.</p> <p>When an alert is received from the Cisco Info Server, by default, it is assigned to a user called <i>nobody</i>. You can manipulate an event that has been assigned either to the user <i>nobody</i>, or one that has been assigned to you. You can also manipulate an alert when it has been assigned to a Cisco Info Center group to which you belong.</p>
Target Platform(s)	Cisco AS5000 series, Cisco 3660
Application	CIC, CEMF
Frequency	As needed

Reference

[Cisco Info Center User Guide](#)

For all related documentation, see [References](#), page 6-2.

Procedure

To manage events using the Event List:

-
- Step 1** In the above reference, refer to Chapter 2, “Using the Event List.”
- Step 2** Read the sections The UNIX Event List and The Java Event List and follow the steps therein.
-

Managing the Cisco Info Server Using CLI Options

Description

Summary	A variety of CLI options are available to manage the Cisco Info Server.
Target Platform(s)	Cisco AS5000 series, Cisco 3660
Application	CIC, CEMF
Frequency	As needed

Reference

Cisco Info Center Administrator Reference

For all related documentation, see [References](#), page 6-2.

Procedure

To manage the Info Server using the CLI options:

-
- Step 1** In the above reference, refer to Chapter 1, “The Info Server.”
- Step 2** Read the section Command Line Options.
- Step 3** As appropriate, follow the steps in one or more of the following:
- Setting the Name of the Cisco Info Server
 - Setting the Process Agent Name
 - Setting the DNS Hostname
 - Specifying the Port
 - Specifying the Properties File
 - Specifying the SQL File
 - Forcing Unique Log Files
 - Setting the Log File Size
 - Naming the Log File
 - Sending Log Output to Standard Error
 - Logging Every Delete
 - Secure Mode Support
 - Statistics

- n. Controlling Updates to Clients
 - a. Controlling Updates of the Database Files on Disk
 - b. Controlling the Automations Clock
 - c. Setting the Maximum Number of Connections
 - d. Setting the Internal Stack Size
 - e. Changing the Queue Size
 - f. Setting the Internal Hash Tables
 - g. Finding out the Version of the Cisco Info Server
 - h. Getting Help on the Cisco Info Server
-

Creating and Editing the Interfaces File

Description

Summary	Communications between the Cisco Info Server and other components, such as Admin Desktops running on separate hosts, is controlled by entries in the interfaces file in the <i>/opt/Omnibus/etc</i> directory. This file can be edited directly or by using the nco_xigen utility. The interfaces file is created automatically when you run the nco_config configuration utility to configure the Info Server and other components. After running nco_config during the initial installation procedure, you can modify the interfaces as needed by running the nco_xigen utility.
Target Platform(s)	Cisco AS5000 series, Cisco 3660
Application	CIC, CEMF
Frequency	As needed

Reference

Cisco Info Center Installation and Configuration

For all related documentation, see [References](#), page 6-2.

Procedure

To modify the interfaces file using the **nco_config** configuration utility:

-
- Step 1** In the above reference, refer to Chapter 6, “Installation Utilities.”
 - Step 2** Reading the sections Interfaces File and Running the **nco_xigen** Utility.
 - Step 3** As appropriate, follow the steps in one or more of the following tasks in Adding a Backup Server.
 - a. Changing the Priority of the Servers
 - b. Adding a New Server
 - c. Changing the Server Details
 - d. Deleting a Serve
 - e. Testing the Server
-

Managing Objects Using the Objective View

Description

Summary	The Objective View displays map books, which contain a number of layered map pages, which in turn are made up of layers, which in turn contain graphical objects called symbols. From these symbols you can display the status of entities, move to another map page, show an Event List, or run a tool.
Target Platform(s)	Cisco AS5000 series, Cisco 3660
Application	CIC, CEMF
Frequency	As needed

Reference

Cisco Info Center User Guide

For all related documentation, see [References, page 6-2](#).

Procedure

To display the status of objects or entities using the Objective View Window of the conductor CIC component:

-
- Step 1** In the above reference, refer to Chapter 5, “Using the Objective View.”
- Step 2** Read the sections Introduction to the Objective View and Starting the Objective View.
- Step 3** As appropriate, follow the steps in one or more of the following:
- Displaying a Map Page
 - Showing the Severity Colors
 - Displaying Map Page Layers
 - Refreshing the Display
 - Displaying the Panner
 - Status Display in a Map Page
 - Actions in a Map Page
-

Managing User Access

Description

Summary	The Users tab on the Configuration Manager window allows you to view and edit the user and groups list on a specific Info Server. Users are administered on a per Info Server basis. If multiple Info Servers are in use, changes on one Info Server do not affect other Info Servers.
Target Platform(s)	Cisco AS5000 series, Cisco 3660
Application	CIC, CEMF
Frequency	As needed

Reference

Cisco Info Center User Guide

For all related documentation, see [References, page 6-2](#).

Procedure

To view and edit the user and groups list on a specific Info Server:

-
- Step 1** In the above reference, refer to Chapter 4, “User Administration.”
 - Step 2** Read the sections User Administration, System Users, and Groups.
 - Step 3** As appropriate, follow the steps in one or more of the following:
 - a. Starting User Administration
 - b. Creating and Editing Users
 - c. Deleting Users
 - d. Adding a User to a Group
 - e. Creating and Renaming Groups
 - f. Deleting Groups
 - g. Adding Users to a Group
 - h. Removing Users
-

Creating, Editing, and Managing Filters Using the Filter Builder

Description

Summary	The Filter Builder is a window used to create, edit, and manage filters. Filters are used to display only those alerts you want to see.
Target Platform(s)	Cisco AS5000 series, Cisco 3660
Application	CIC, CEMF
Frequency	As needed

Reference

Cisco Info Center User Guide

For all related documentation, see [References, page 6-2](#).

Procedure

To create or edit filters using the Filter Builder:

-
- Step 1** In the above reference, refer to Chapter 3, “Filtering Alerts.”
- Step 2** Read and follow the steps in the following sections:
- Creating Condition Elements
 - Creating Logical Elements
 - Creating Subquery Elements
 - Deleting Elements
 - Copying and Pasting Elements
 - Saving Filters
 - Loading Filters
 - Drag and Drop Filters
-

Creating, Editing, and Managing Views Using View Builder

Description

Summary	Use View Builder to create, edit, and manage views.
Target Platform(s)	Cisco AS5000 series, Cisco 3660
Application	CIC, CEMF
Frequency	As needed

Reference

Cisco Info Center User Guide

For all related documentation, see [References, page 6-2](#).

Procedure

To use View Builder to create, edit, and manage views:

-
- | | |
|---------------|---|
| Step 1 | In the above reference, refer to Chapter 4, “View Builder.” |
| Step 2 | Read the sections Introduction to the View Builder, Changing the Appearance of the View, Saving Views, Loading Views, and Dragging and Dropping Views, and follow the instructions therein as needed. |
-

Troubleshooting: Using CIC Diagnostic Tools

Description

Summary	CIC incorporates Cisco element managers, diagnostics, and troubleshooting tools into the fault management environment. Tools are context sensitive, depending on the type of alarm being addressed or the label of the object displayed. Tools available from CIC menus include the following: CiscoView for Cisco WAN Manager Equipment Management, Administration GUI, Get Configuration, Real Time Counters, Test Delay, Test Connection, Add Loopback, Delete Loopback, Decode BitMap, Create Event List, Desktop Information, HP Network Node Manager, and Cisco WAN Manager Desktop.
Target Platform(s)	Cisco AS5000 series, Cisco 3660
Application	CIC, CEMF
Frequency	As needed

Reference

Cisco Info Center User Guide. See [References, page 6-2](#). See in particular Appendix D, “Cisco Info Center Diagnostic Tools,” at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/info_ctr/3_0/user_gd/app_diag.htm

Procedure

To use CIC diagnostic tools:

-
- Step 1** In the *Cisco Info Center User Guide*, refer to Appendix D, “Cisco Info Center Diagnostic Tools.”
 - Step 2** Read the sections applicable to the troubleshooting and diagnostic tasks you want to accomplish, and follow the instructions therein.
-



Operating and Maintaining the Cisco Access Registrar

Introduction

This chapter presents operations and maintenance tasks for the application Cisco Access Registrar (AR), Release 1.7, as it relates to the Cisco ASAP Solution only.



Note

This chapter *does not apply* to the PSTN gateway solutions.

Tips for troubleshooting Cisco AR are provided in [Chapter 14, “Troubleshooting the Cisco Access Registrar.”](#)

Cisco AR supports RADIUS proxy where, instead of directly authenticating and authorizing users against a directory, the server selectively proxies the AAA request to another service provider's RADIUS server or a customer RADIUS server that authenticates and authorizes users against another directory or database.

This chapter presents the following major operations and maintenance topics:

- [Installing and Upgrading the Cisco AR](#)
- [Configuring a Basic Site](#)
- [Making Custom Configurations](#)
- [Performing Maintenance and Management Tasks](#)



Tip

See also [Task Summary, page 7-2](#).

Target Platforms

The Cisco Access Registrar application manages the following components of the Cisco ASAP Solution: Cisco AS5000 series.

References

For detailed information about how to install and configure the Cisco AR, see the *Cisco Access Registrar 1.7 Installation and Configuration Guide*:

http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cnsar/1_7/install/index.htm

For description of the Cisco AR components and how to use them, including information of how to use the Cisco AR as a proxy server and details about the using the **aregcmd** and **radclient** commands, refer to the *Cisco Access Registrar 1.7 User's Guide* at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cnsar/1_7/users/index.htm

For description of the concepts in the Cisco AR, including understanding RADIUS, authentication and authorization, and accounting refer to the *Cisco Access Registrar 1.7 Concepts and Reference Guide* at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cnsar/1_7/referenc/index.htm

For description of features and functions that were implemented in the Cisco AR Release 1.7, refer to the *Cisco Access Registrar 1.7 Release Notes*:

http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cnsar/1_7/relnote/index.htm

Task Summary

The tasks in this chapter are listed below, grouped by major category.

Installing and Upgrading the Cisco AR

To either install or upgrade the Cisco AR, you have the follow options:

- Upgrade from an earlier version of Cisco AR and erase your previous configuration
- Upgrade from an earlier version of Cisco AR and retain your previous configuration
- Install AR on a system for the first time

For detailed procedures of how to implement any of these options, refer to Chapter 1, “Installing Cisco Access Registrar” and Chapter 2, “Upgrading Cisco Access Registrar,” of the *Cisco Access Registrar 1.7 Installation and Configuration Guide*.

Configuring a Basic Site

- [Configuring Clients](#)
- [Configuring Profiles](#)
- [Validating Configurations](#)

Making Custom Configurations

- [Configuring Groups](#)
- [Configuring Multiple UserLists](#)
- [Configuring a Remote Server](#)
- [Configuring Session Management](#)

Performing Maintenance and Management Tasks

- [Checking the AR Server](#)
- [Logging in to the Cisco AR](#)
- [Configuring, Modifying, and Managing Syslog Messages](#)
- [Managing the Cisco AR Using aregcmd Commands](#)
- [Modifying Configurations Using aregcmd Commands](#)
- [Setting Up and Managing Accounting](#)
- [Backing Up the Database](#)
- [Monitoring the UG](#)

Configuring Clients

Description

Summary	The Clients object contains all NASs (UGs) and proxies that communicate directly with Cisco AR. Each client must have an entry in the Clients list, because each NAS and proxy share a secret with the RADIUS server, which is used to encrypt passwords and sign responses.
Target Platform(s)	Cisco AS5000 series
Application	Cisco AR
Frequency	When installing Cisco AR for the first time

Reference

Cisco Access Registrar 1.7 Installation and Configuration Guide

For all related documentation, see [References](#), page 7-2.

Procedure

To configure the Client object and a NAS for the Cisco AR:

-
- | | |
|---------------|--|
| Step 1 | In the above reference, see Chapter 3, “Configuring Cisco Access Registrar.” |
| Step 2 | Read the section Configuring Clients and follow the steps to add NASs. |
-

Notes

- *Related documents:* For information about the Access Registrar Server objects, including the Client object, see Chapter 3, “Access Registrar Server Objects,” of the *Cisco Access Registrar 1.7 User's Guide*.

Configuring Profiles

Description

Summary	The Profiles object allows you to set specific RFC-defined attributes that Cisco AR returns in the Access-Accept response. You can use profiles to group attributes that belong together.
Target Platform(s)	Cisco AS5000 series
Application	Cisco AR
Frequency	When configuring Cisco AR for the first time or modifying existing configurations when necessary

Reference

Cisco Access Registrar 1.7 Installation and Configuration Guide

For all related documentation, see [References](#), page 7-2.

Procedure

For adding or modifying RADIUS attributes:

-
- | | |
|---------------|--|
| Step 1 | In the above reference, see Chapter 3, “Configuring Cisco Access Registrar,” of the <i>Cisco Access Registrar 1.7 User’s Guide</i> . |
| Step 2 | Read the section Configuring Profiles and follow the steps to change RADIUS attributes. |
-

Validating Configurations

Description

Summary	<p>The aregcmd commands are command-line based configuration tools. These commands allow you to set any Cisco AR configuration option, as well as start and stop the Cisco AR RADIUS server and check its statistics.</p> <p>The radclient command is a RADIUS server test tool. It enables you to create packets, send them to a specific server, and examine the response.</p> <p>Use the save and reload of the aregcmd commands to save and reload the configuration changes you made. Use the radclient command to send a test packet.</p>
Target Platform(s)	Cisco AS5000 series
Application	Cisco AR
Frequency	When installing Cisco AR for the first time

Reference

Cisco Access Registrar 1.7 User's Guide

For all related documentation, see [References, page 7-2](#).

Procedure

Once you have configured some users and a NAS, you can validate and test your configuration as follows:

-
- | | |
|---------------|---|
| Step 1 | Use the save command to save your changes. |
| Step 2 | Use the reload command to reload your server. |
| Step 3 | Run the radclient command to send a test packet. |
| Step 4 | For syntax and description of these command, see Chapter 2, "Using aregcmd Commands," and Chapter 4, "Using the radclient Command," of the <i>Cisco Access Registrar 1.7 User's Guide</i> . |
-

Notes

- *Related documents:* For information about all the **aregcmd** commands and their syntax description, see Chapter 2, "Using aregcmd Commands," of the *Cisco Access Registrar 1.7 User's Guide*.

Configuring Groups

Description

Summary	To create user groups for the services that you want to provide, use the UserGroups object. You can either use the default group (and depending how the user logs, use a script to determine the services you want to provide to that user), or you can create separate groups for each specific type of service (for example, one group for PPP users and another for Telnet users).
Target Platform(s)	Cisco AS5000 series
Application	Cisco AR
Frequency	As needed

Reference

Cisco Access Registrar 1.7 Installation and Configuration Guide

For all related documentation, see [References](#), page 7-2.

Procedure

To configure groups:

-
- | | |
|---------------|--|
| Step 1 | In above reference, see Chapter 4, “Customizing Your Site.” |
| Step 2 | Read the section Configuring Groups. |
| Step 3 | As appropriate, follow the steps in one or more of the following sections: <ol style="list-style-type: none">Configuring Specific GroupsConfiguring a Default Group |
-

Notes

- *Related documents:* For information about the Cisco Access Registrar Server objects, including the Group object, see Chapter 3, “Access Registrar Server Objects,” of the *Cisco Access Registrar 1.7 User's Guide*.

Configuring Multiple UserLists

Description

Summary	The basic site uses a default single UserList and uses group membership to determine the type of service to provide each user. When all users are in the same UserList, each username must be unique. Another option you have is to group your user community some logical grouping like department or location. In this method you use separate UserLists to distinguish among them.
Target Platform(s)	Cisco AS5000 series
Application	Cisco AR
Frequency	As needed

Reference

Cisco Access Registrar 1.7 Installation and Configuration Guide

For all related documentation, see [References](#), page 7-2.

Procedure

To configure multiple UserLists:

-
- Step 1** In the above reference, see Chapter 4, “Customizing Your Site.”
 - Step 2** Read the section Configuring Multiple UserLists.
 - Step 3** As appropriate, follow the steps in one or more of the following sections:
 - a. Configuring Separate UserLists
 - b. Configuring Users
 - c. Configuring Services
 - d. Creating the Script
 - e. Configuring the Script
-

Notes

- *Related documents:* For information about the Cisco Access Registrar Server objects, including the UserLists object, see Chapter 3, “Access Registrar Server Objects,” of the *Cisco Access Registrar 1.7 User's Guide*.

Configuring a Remote Server

Description

Summary	If you want to divide the tasks of authentication and authorization to another RADIUS server or an LDAP server, you use the RemoteServer object to specify the properties of the remote server to which Services proxy requests are sent. The remote servers you specify at this level are referenced by name from the RemoteServers list in the Services objects.
Target Platform(s)	Cisco AS5000 series
Application	Cisco AR
Frequency	As needed

Reference

Cisco Access Registrar 1.7 Installation and Configuration Guide

For all related documentation, see [References](#), page 7-2.

Procedure

To configure a remote RADIUS server:

-
- | | |
|---------------|--|
| Step 1 | In the above reference, see Chapter 4, “Customizing Your Site.” |
| Step 2 | Read the section Configuring a Remote Server for AAA. |
| Step 3 | As appropriate, follow the steps in one or more of the following sections: <ol style="list-style-type: none">Configuring the Remote ServerConfiguring ServicesChanging the Authentication and Authorization DefaultsConfiguring Two Remote ServersConfiguring the Script |
-

Notes

- Related documents:* For information about the Cisco Access Registrar Server objects, see Chapter 3, “Access Registrar Server Objects,” of the *Cisco Access Registrar 1.7 User's Guide*.

Configuring Session Management

Description

Summary	Session management can be used to track user sessions and allocate dynamic resources to users for the lifetime of their sessions. You can define one or more Session Managers, and have each one manage the sessions for a particular group or company.
Target Platform(s)	Cisco AS5000 series
Application	Cisco AR
Frequency	As needed

Reference

Cisco Access Registrar 1.7 Installation and Configuration Guide

For all related documentation, see [References](#), page 7-2.

Procedure

To configure session management on the Cisco AR:

-
- Step 1** In the above reference, see Chapter 4, “Customizing Your Site.”
 - Step 2** Read the section Configuring Session Management.
 - Step 3** As appropriate, follow the steps in one or more of the following sections:
 - a. Creating a Resource Manager
 - b. Configuring a Session Manager
 - c. Enabling Session Management
-

Checking the AR Server

Description

Summary	After installation of the Cisco AR, you can verify that the server is running correctly with the arstatus command. Successfully running this command ensures that you can communicate with the database, communicate with the RADIUS server, and determine whether the server is running or stopped.
Target Platform(s)	Cisco AS5000 series
Application	Cisco AR
Frequency	When installing Cisco AR for the first time or as needed.

Reference

Cisco Access Registrar 1.7 Installation and Configuration Guide

For all related documentation, see [References](#), page 7-2.

Procedure

To check if the Cisco AR servers are running:

-
- Step 1** Enter the **arstatus** command in interactive mode:
- ```
>arstatus
RADIUS server running (pid: 649)
MCD server running (pid: 648)
Server Agent running (pid: 647)
MCD Lock Manager running (pid: 651)
```
- Step 2** If the servers are not running, do the following:
- Become superuser (**su**).
  - Change to the **/etc/init.d** directory.
  - Type the **arservagt** command with the **start** argument:  

```
>.arservagt start
```
-

# Logging in to the Cisco AR

## Description

|                           |                                                                             |
|---------------------------|-----------------------------------------------------------------------------|
| <b>Summary</b>            | After verifying that the Cisco AR is running, you can log in to the server. |
| <b>Target Platform(s)</b> | Cisco AS5000 series                                                         |
| <b>Application</b>        | Cisco AR                                                                    |
| <b>Frequency</b>          | When installing Cisco AR for the first time or as needed                    |

## Reference

[Cisco Access Registrar 1.7 Installation and Configuration Guide](#)

For all related documentation, see [References, page 7-2](#).

## Procedure

To log into the Cisco AR server:

- 
- Step 1** Enter the **aregcmd** command in interactive mode:
  - Step 2** The Cisco Access Registrar prompts you for the cluster. Type the cluster name or press **Enter** for **localhost**.
  - Step 3** The Cisco AR prompts you for the **admin** login and password. Use **admin** for the admin name, and **aicuser** for the password.
  - Step 4** The Cisco AR prompts you to enter a valid license key. Enter the license key that is located on the back of the Cisco Access Registrar CD case.
- 

## Notes

- *Related documents:* For information about all the **aregcmd** commands and their syntax description, see Chapter 2, “Using aregcmd Commands,” of the *Cisco Access Registrar 1.7 User’s Guide*.

# Configuring, Modifying, and Managing Syslog Messages

## Description

|                           |                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|---------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Summary</b>            | Logging messages through syslog provides centralized error reporting for Cisco AR. Local logging and syslog logging can be turned on or off at any time by modifying the control flags in the <code>\$INSTALLPATH/conf/aic.conf</code> file.<br><br>Logging syslog messages requires a UNIX host running a <code>syslog daemon</code> as a receiver for Cisco AR messages. The Cisco AR and the syslog daemon can be running on the same host or different hosts. |
| <b>Target Platform(s)</b> | Cisco AS5000 series                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>Application</b>        | Cisco AR                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>Frequency</b>          | As needed                                                                                                                                                                                                                                                                                                                                                                                                                                                         |

## Reference

[Cisco Access Registrar 1.7 User's Guide](#)

For all related documentation, see [References](#), page 7-2.

## Procedure

To configure, modify, or manage syslog messages for the Cisco AR:

- 
- Step 1** In the above reference, see Chapter 13, “Logging Syslog Messages”.
- Step 2** Read the sections Configuring Message Logging, Changing Log Directory, Configuring syslog Daemon (syslogd), and Managing the Syslog File.
- Step 3** As appropriate, follow the steps in one or more of the following:
- Creating a Log File
  - Restarting syslogd
  - Managing the Syslog File
-

# Setting Up and Managing Accounting

## Description

|                           |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|---------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Summary</b>            | The Cisco AR collects and stores the information contained in Accounting Start and Accounting Stop messages.<br><br>When a NAS (UG) that uses accounting begins a session, it sends an Accounting Start packet describing the type of service and the user being connected to the Cisco AR server. When the session ends, the NAS sends an Accounting Stop packet to the AR server describing the type of service that was delivered. The Accounting Stop packet might also contain statistics such as elapsed time, input and output octets, or input and output packets. |
| <b>Target Platform(s)</b> | Cisco AS5000 series                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Application</b>        | Cisco AR                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>Frequency</b>          | As needed                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |

## Reference

*Cisco Access Registrar 1.7 Concepts and Reference Guide*

For all related documentation, see [References](#), page 7-2.

## Procedure

To set up and manage accounting using Cisco AR:

- 
- Step 1** In the above reference, refer to Chapter 3, “Access Registrar Accounting.”
  - Step 2** Read the sections Understanding Access Registrar Accounting, Setting Up Accounting, and Accounting Log File Rollover.
  - Step 3** As appropriate, follow the steps in one or more of the following:
    - a. Setting Up Accounting
    - b. Configuring Accounting
-

# Modifying Configurations Using aregcmd Commands

## Description

|                           |                                                                                                                                                                                                                           |
|---------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Summary</b>            | The <b>aregcmd</b> commands are command-line based configuration tools. These commands allow you to set any Cisco AR configuration option, as well as start and stop the Cisco AR RADIUS server and check its statistics. |
| <b>Target Platform(s)</b> | Cisco AS5000 series                                                                                                                                                                                                       |
| <b>Application</b>        | Cisco AR                                                                                                                                                                                                                  |
| <b>Frequency</b>          | As needed                                                                                                                                                                                                                 |

## Reference

*Cisco Access Registrar 1.7 User's Guide*

For all related documentation, see [References](#), page 7-2.

**Note**

---

For the syntax and description of these commands, see Chapter 2, “Using aregcmd Commands,” of the *Cisco Access Registrar 1.7 User's Guide*.

---

## Procedure

To modify existing configuration of the Cisco AR or to modify values for properties, use the following **aregcmd** commands:

- 
- Step 1** Use the **add** command to add elements to your configuration.
  - Step 2** use the **delete** command to remove an element from the configuration.
  - Step 3** Once you made changes to the your configuration, use **save** and **reload** commands to implement the changes you made.
  - Step 4** Use the **set** command to provide values for properties on existing configuration elements or to order servers in a list.
  - Step 5** Use the **unset** command to remove items from an ordered list.
  - Step 6** Use the **insert** command to add an item anywhere in ordered list.
-

# Managing the Cisco AR Using aregcmd Commands

## Description

|                           |                                                                                                                                                                                                                            |
|---------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Summary</b>            | The <b>aregcmd</b> commands are command-line based configuration tools. These commands allow you to set any Cisco AR configuration option, as well as, start and stop the Cisco AR RADIUS server and check its statistics. |
| <b>Target Platform(s)</b> | Cisco AS5000 series                                                                                                                                                                                                        |
| <b>Application</b>        | Cisco AR                                                                                                                                                                                                                   |
| <b>Frequency</b>          | As needed                                                                                                                                                                                                                  |

## Reference

*Cisco Access Registrar 1.7 User's Guide*

For all related documentation, see [References, page 7-2](#).



### Note

For the syntax and description of these commands, see Chapter 2, “Using aregcmd Commands,” of the *Cisco Access Registrar 1.7 User's Guide*.

## Procedure

To manage your Cisco AR server, use the following **aregcmd** commands:

- 
- Step 1** Use the **insert** command to add an item anywhere in ordered list.
  - Step 2** Use **save** command to validate the changes you made and commit them to the configuration database.
  - Step 3** Use the **validate** command to check the consistency and validity of the specified server's configuration.
  - Step 4** Use the **start** command to enable the server to handle requests.
  - Step 5** Use the **stop** command to stop server from accepting requests.
  - Step 6** Use the **reload** command to load the configuration changes.
  - Step 7** Use the **status** command to see whether or not the specified server has been started.
  - Step 8** Use the **stat** command to view statistical information on the specified server.
  - Step 9** Use the **query-sessions** command to query the server about the currently active user sessions.
  - Step 10** Use the **release-sessions** to request the server to release one or more currently active user sessions.
  - Step 11** Use the **help** command to display a brief overview of the command syntax.
-



# Backing Up the Database

## Description

|                           |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|---------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Summary</b>            | .To ensure a consistent backup, Cisco AR uses a shadow backup facility. Once a day, at a configurable time, Cisco AR suspends all activity to the database, and takes a snapshot of the critical files. This snapshot is guaranteed to be a consistent view of the database, and it is preserved correctly on a system backup tape. The backup can be do either through the system Registry at <i>\$INSTALL/conf/aic.conf</i> or using <b>mcshadow</b> utility located in the <i>\$INSTALL1/usrbin</i> directory. |
| <b>Target Platform(s)</b> | Cisco AS5000 series                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>Application</b>        | Cisco AR                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>Frequency</b>          | As needed                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |

## Reference

*Cisco Access Registrar 1.7 User's Guide*

For all related documentation, see [References](#), page 7-2.

## Procedure

To back up the Access Registrar database either using a configurable time or using the **mcshadow** utility:

- 
- Step 1** In the above reference, refer to Chapter 12, “Backing Up the Database.”
- Step 2** Read and follow the steps in the following sections:
- Configuration
  - Recovery
-

# Monitoring the UG

## Description

|                           |                                                                                                                                                                                                                                                                                                                                                                                           |
|---------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Summary</b>            | The <b>nasmonitor</b> command is used to query a TCP port at the specified IP address until the device (universal gateway) is reachable. If the universal gateway (UG) is not reachable after period of time, a warning E-mail is sent; if the UG is still not reachable after another period of time, a message is sent to the Cisco AR to release all sessions associated with that UG. |
| <b>Target Platform(s)</b> | Cisco AS5000 series universal gateways                                                                                                                                                                                                                                                                                                                                                    |
| <b>Application</b>        | Cisco AR                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>Frequency</b>          | As needed.                                                                                                                                                                                                                                                                                                                                                                                |

## Reference

[Cisco Access Registrar 1.7 User's Guide](#)

For all related documentation, see [References, page 7-2](#).

## Procedure

To check if NAS (UG) is reachable by the Cisco AR use the following **nasmonitor** command:

- 
- |               |                                                                                             |
|---------------|---------------------------------------------------------------------------------------------|
| <b>Step 1</b> | In the above reference, refer to Chapter 8, "Using Cisco Access Registrar Server Features." |
| <b>Step 2</b> | Read the section NAS Monitor and follow the steps.                                          |
-



# Using Cisco IOS for Operations and Maintenance

## Introduction

This chapter presents operations and maintenance tasks related to the Cisco ASAP Solution and the PSTN gateway solutions that are provided by Cisco IOS commands entered at the command-line interface (CLI).

This chapter presents the following major topics:

- [Monitoring Network Performance Using IOS Commands](#)
- [Managing Gateways](#)
- [Managing Gatekeepers](#)
- [Managing Modems](#)
- [Using MIB Objects](#)
- [Cisco IOS References](#)



**Tip**

---

See also [Task Summary, page 8-2](#).

---

## Target Platforms

The Cisco IOS CLI manages the following components of the Cisco ASAP Solution and the PSTN gateway solutions: Cisco AS5000 series.

## References

See [Cisco IOS References, page 8-12](#).

## Task Summary

The tasks in this chapter are listed below, grouped by major category.

### Monitoring Network Performance

- [Monitoring Network Performance Using IOS Commands](#)

### Managing Gateways

- [Checking Memory and CPU Utilization](#)
- [Configuring Call Admission Control Thresholds Using Cisco IOS Commands](#)
- [Verifying Call Admission Control Configurations](#)
- [Verifying Controllers](#)
- [Verifying ISDN PRI](#)
- [Verifying ISDN D-Channels](#)
- [Verifying Universal Port Card and Lines](#)
- [Verifying Clocking](#)
- [Testing Asynchronous Shell Connections](#)
- [Configuring and Verifying Alarms](#)
- [Managing and Viewing SPE Performance Statistics](#)
- [Managing Ports](#)
- [Managing and Troubleshooting SPEs](#)
- [Using Cisco Call Tracker to Manage Gateways](#)

### Managing Gatekeepers

- [Configuring Load Balancing and Alternate Gatekeepers](#)
- [Configuring Remote Clusters](#)
- [Configuring Server Triggers](#)
- [Verifying Gatekeeper Configuration](#)
- [Maintaining and Monitoring Gatekeeper Endpoints](#)

### Managing Modems

- [Managing Modems](#)

### Using MIB Objects

- [Using MIB Objects](#)

# Monitoring Network Performance Using IOS Commands

The performance of a network is directly linked to the operational state of devices within the network. The hardware and software components of a network device also affect its performance. Failed hardware components can cause a complete outage in the network. It is critical to monitor the operating environments of network devices, such as voltage, temperature, and airflow, and ensure that they are operating within specifications. Software components such as buffers and memory can have a significant impact on the protocols running on the device.

A useful performance indicator on the Cisco devices is their CPU utilization. By measuring CPU utilization over time, a trend can be established to determine traffic patterns. Devices running constantly at high utilization levels can affect the overall performance of forwarding and processing packets. CLI commands on the Cisco devices can display the CPU utilization and information on running processes. Information returned on the CPU load can be accessed by means of objects defined in MIB files. For details on using such files, see [Using MIB Objects, page 8-12](#).

## Managing Gateways

For a good discussion of a variety of ways to verify basic setups, as well to determine memory and CPU utilization, refer to *Cisco AS5350 and Cisco AS5400 Universal Gateway Software Configuration Guide* at the following URL:

[http://www.cisco.com/univercd/cc/td/doc/product/access/acs\\_serv/as5350/sw\\_conf/53swcg/index.htm](http://www.cisco.com/univercd/cc/td/doc/product/access/acs_serv/as5350/sw_conf/53swcg/index.htm)

Consider, in particular, the following topics.

## Checking Memory and CPU Utilization

The basic command to see CPU utilization is **show processes**. The following example displays results of that command:

```
Router# show processes
CPU utilization for five seconds: 1%/0%; one minute: 1%; five minutes: 1%
```

| PID | QTy | PC       | Runtime (ms) | Invoked | uSecs | Stacks    | TTY | Process         |
|-----|-----|----------|--------------|---------|-------|-----------|-----|-----------------|
| 1   | Mwe | 6039CCC8 | 2203448      | 9944378 | 221   | 7392/9000 | 0   | IP-EIGRP Router |
| 2   | Lst | 60133594 | 329612       | 34288   | 9613  | 5760/6000 | 0   | Check heaps     |
| 3   | Cwe | 6011D820 | 0            | 1       | 0     | 5648/6000 | 0   | Pool Manager    |
| 4   | Mst | 6015FAA8 | 0            | 2       | 0     | 5608/6000 | 0   | Timers          |

You can also use a MIB to monitor the output of this command. [Table 8-3 on page 8-12](#) provides the MIB objects in the OLD-CISCO-CPU-MIB for monitoring the output of a **show processes** command.

The amount of main memory left on the processor of a device has a significant impact on performance. Buffers are allocated from memory into different memory pools that are used by a protocol. The following CLI commands are commonly used to monitor the memory and buffer statistics on a device: **show memory**, **show buffers**, and **show interface**.

The following example displays the memory allocation resulting from the the **show memory** command.

```
Router# show memory
Head Total(b) Used(b) Free(b) Lowest(b) Largest(b)
Processor 60DB19C0 119858752 1948928 117909824 117765180 117903232
Fast 60D919C0 131072 69560 61512 61512 61468
```

There is a MIB that allows you to capture the output of this command. [Table 8-4 on page 8-12](#) provides the MIB objects in the CISCO-MEMORY-POOL-MIB for monitoring the output of a **show memory** command.

**Note**

Refer to *Cisco AS5350 and Cisco AS5400 Universal Gateway Software Configuration Guide* at the following URL:

[http://www.cisco.com/univercd/cc/td/doc/product/access/acs\\_serv/as5350/sw\\_conf/53swcg/index.htm](http://www.cisco.com/univercd/cc/td/doc/product/access/acs_serv/as5350/sw_conf/53swcg/index.htm)

Note Chapter 2, “Verifying Basic Setup,” and the following sections therein:

Investigating Memory Usage Illustrates the command **show memory summary**. Inspecting CPU Utilization illustrates the command **show process cpu history**.

## Configuring Call Admission Control Thresholds Using Cisco IOS Commands

[Table 8-1](#) lists the high-level tasks that you need to complete for configuring Call Admission Control (CAC) thresholds.

For step-by-step instructions, refer to the documentation for the following feature modules, at their respective URLs:

- Call Admission Control for H.323 VoIP Gateways at the following URL:

[http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122limit/122x/122xa/122xa\\_2/ft\\_pfavb.htm](http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122limit/122x/122xa/122xa_2/ft_pfavb.htm)

- Call Admission Control Based on CPU Utilization at the following URL:

[http://www.cisco.com/univercd/cc/td/doc/product/access/acs\\_serv/as5800/sw\\_conf/ios\\_122/dt61294.htm](http://www.cisco.com/univercd/cc/td/doc/product/access/acs_serv/as5800/sw_conf/ios_122/dt61294.htm)

**Table 8-1 Tasks for Configuring Call Admission Control Thresholds**

| Tasks                                    | Description                                                                                                                                                                                                             |
|------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Configuring Call Spike                   | Configures the limit for the number of incoming calls in a short period of time.                                                                                                                                        |
| Configuring Call Threshold               | Enables a resource and defines associated parameters. Action is enabled when the resource cost goes beyond the <b>high value</b> and is not disabled until the resource cost drops below the <b>low value</b> .         |
| Configuring Call Threshold Poll-Interval | Enables a polling interval threshold for CPU or memory.                                                                                                                                                                 |
| Configuring Call Treatment               | Configures how calls should be processed when local resources are unavailable. This indicates whether the call should be disconnected (with cause code), hairpinned, or should play a message or busy tone to the user. |
| Configuring Call Denial                  | Enters the Call Denial feature and sets a threshold at which denial of new calls occurs. This CPU load threshold can be set anywhere from 20 to 85%.                                                                    |

## Verifying Call Admission Control Configurations

To verify the Call Admission Control configuration tasks, enter the following commands in privileged EXEC mode.

| Command                       | Description                                                                                                                                                                      |
|-------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>show call spike status</b> | Displays the configured call spike threshold and statistics for incoming calls.                                                                                                  |
| <b>show call threshold</b>    | Displays enabled triggers, current values for configured triggers, and number of Application Programming Interface (API) calls that were made to global and interface resources. |
| <b>show call treatment</b>    | Displays the call treatment configuration and the statistics for handling the calls based upon resource availability.                                                            |
| <b>show process</b>           | Displays the CPU threshold value configured for call denial.                                                                                                                     |
| <b>show running-config</b>    | Displays all of the configurations                                                                                                                                               |

## Verifying Controllers

Refer to *Cisco AS5350 and Cisco AS5400 Universal Gateway Software Configuration Guide* at the following URL:

[http://www.cisco.com/univercd/cc/td/doc/product/access/acs\\_serv/as5350/sw\\_conf/53swcg/index.htm](http://www.cisco.com/univercd/cc/td/doc/product/access/acs_serv/as5350/sw_conf/53swcg/index.htm)

In the above-referenced guide, refer to Chapter 3, “Basic Configuration Using the Command-Line Interface,” and the following sections therein:

- Configuring the Asynchronous Group Interface  
Refer to the subsection Verify in the above section, which illustrates the commands **show interface async 4/0** and **show async status**.
- Configuring Channelized T1 and E1 Feature Cards  
Refer to the subsection Verify in the above section, which illustrates the command **show controller**.
- Configuring Channelized T3 Feature Card  
Refer to the subsection Verify in the above section, which illustrates the command **show controller**.

## Verifying ISDN PRI

Refer to *Cisco AS5350 and Cisco AS5400 Universal Gateway Software Configuration Guide* at the following URL:

[http://www.cisco.com/univercd/cc/td/doc/product/access/acs\\_serv/as5350/sw\\_conf/53swcg/index.htm](http://www.cisco.com/univercd/cc/td/doc/product/access/acs_serv/as5350/sw_conf/53swcg/index.htm)

In the above-referenced guide, refer to Chapter 3, “Basic Configuration Using the Command-Line Interface,” and the following sections therein:

- Configuring ISDN PRI  
Refer to the subsection Verify in the above section, which illustrates the following commands: **show controller t3**, **show isdn status**, **show isdn service**, and **show running-config**.

## Verifying ISDN D-Channels

Refer to *Cisco AS5350 and Cisco AS5400 Universal Gateway Software Configuration Guide* at the following URL:

[http://www.cisco.com/univercd/cc/td/doc/product/access/acs\\_serv/as5350/sw\\_conf/53swcg/index.htm](http://www.cisco.com/univercd/cc/td/doc/product/access/acs_serv/as5350/sw_conf/53swcg/index.htm)

In the above-referenced guide, refer to Chapter 3, “Basic Configuration Using the Command-Line Interface,” and the following sections therein:

- Configuring the D Channels for ISDN Signaling

Refer to the subsection Verify in the above section, which illustrates the command **show interface serial**.

## Verifying Universal Port Card and Lines

Refer to *Cisco AS5350 and Cisco AS5400 Universal Gateway Software Configuration Guide* at the following URL:

[http://www.cisco.com/univercd/cc/td/doc/product/access/acs\\_serv/as5350/sw\\_conf/53swcg/index.htm](http://www.cisco.com/univercd/cc/td/doc/product/access/acs_serv/as5350/sw_conf/53swcg/index.htm)

In the above-referenced guide, refer to Chapter 3, “Basic Configuration Using the Command-Line Interface,” and the following sections therein:

- Configuring the Universal Port Card and Lines

Refer to the subsection Verify in the above section, which illustrates the commands **show spe** and **show line**.

Also refer to Chapter 5, “Managing and Troubleshooting the Universal Port Card,” in the same document.

## Verifying Clocking

Refer to *Cisco AS5350 and Cisco AS5400 Universal Gateway Software Configuration Guide* at the following URL:

[http://www.cisco.com/univercd/cc/td/doc/product/access/acs\\_serv/as5350/sw\\_conf/53swcg/index.htm](http://www.cisco.com/univercd/cc/td/doc/product/access/acs_serv/as5350/sw_conf/53swcg/index.htm)

In the above-referenced guide, refer to Chapter 3, “Basic Configuration Using the Command-Line Interface,” and the following sections therein:

- Configuring Clocking

This section illustrates the use of the **at** command **atdt** and the Cisco IOS command **show caller**. You can also use the command **show user**.

## Testing Asynchronous Shell Connections

Refer to *Cisco AS5350 and Cisco AS5400 Universal Gateway Software Configuration Guide* at the following URL:

[http://www.cisco.com/univercd/cc/td/doc/product/access/acs\\_serv/as5350/sw\\_conf/53swcg/index.htm](http://www.cisco.com/univercd/cc/td/doc/product/access/acs_serv/as5350/sw_conf/53swcg/index.htm)

In the above-referenced guide, refer to Chapter 3, “Basic Configuration Using the Command-Line Interface,” and the following sections therein:



- Configuring Clocking

Refer to the subsection Verify in the above section, which illustrates the command **show tdm clocks**.

## Configuring and Verifying Alarms

Refer to *Cisco AS5350 and Cisco AS5400 Universal Gateway Software Configuration Guide* at the following URL:

[http://www.cisco.com/univercd/cc/td/doc/product/access/acs\\_serv/as5350/sw\\_conf/53swcg/index.htm](http://www.cisco.com/univercd/cc/td/doc/product/access/acs_serv/as5350/sw_conf/53swcg/index.htm)

In the above-referenced guide, refer to Chapter 4, “Continuing Configuration Using the Command-Line Interface,” and the following section therein:

- Configuring Alarms



### Caution

By default, facility alarms are off. You must use the command **facility-alarm** and its options to enable alarms related to interfaces, controllers, modem boards, redundant power supplies, temperature, and fans.

Refer to the subsection Verify in the above section, which illustrates the command **show facility-alarm**.

## Managing and Viewing SPE Performance Statistics

Event logs are automatically enabled and are based on one event queue per SPE (system processing engine). The log contains raw binary data that can be viewed by means of a variety of **show spe** commands.

Refer to *Cisco AS5350 and Cisco AS5400 Universal Gateway Software Configuration Guide* at the following URL:

[http://www.cisco.com/univercd/cc/td/doc/product/access/acs\\_serv/as5350/sw\\_conf/53swcg/index.htm](http://www.cisco.com/univercd/cc/td/doc/product/access/acs_serv/as5350/sw_conf/53swcg/index.htm)

In the above-referenced guide, refer to Chapter 5, “Managing and Troubleshooting the Universal Port Card,” and the following sections therein:

- Configuration
- Viewing SPE Performance Statistics

The following command classes, with options, are described: **show spe voice**, **show spe digital**, **show spe modem**, **show port**, and miscellaneous **show spe (log, version, fax)**.

## Managing Ports

In port configuration mode, you can clear ports, remove them from service, or disable them from dial-up service.

Refer to *Cisco AS5350 and Cisco AS5400 Universal Gateway Software Configuration Guide* at the following URL:

[http://www.cisco.com/univercd/cc/td/doc/product/access/acs\\_serv/as5350/sw\\_conf/53swcg/index.htm](http://www.cisco.com/univercd/cc/td/doc/product/access/acs_serv/as5350/sw_conf/53swcg/index.htm)

In the above-referenced guide, refer to Chapter 5, “Managing and Troubleshooting the Universal Port Card,” and the following sections therein:

- Clear Ports
- Port Configuration Mode  
(presents the commands that are available in port configuration mode: **busyout** and **shutdown**)

**Tip**

For the details of port management, including a command reference (applicable to both Cisco AS5350 and Cisco AS5400 platforms), refer to Managing Port Services on the Cisco AS5400 Universal Access Server at the following URL:

<http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t3/nextport/index.htm>

## Managing and Troubleshooting SPEs

In SPE configuration mode, you can transfer firmware from flash memory and specify an upgrade method, minimizing the impact on traffic.

In the above-referenced guide, refer to Chapter 5, “Managing and Troubleshooting the Universal Port Dial Feature Card,” and the following sections therein:

- SPE Configuration Mode  
Presents the SPE management options that are available in SPE configuration mode: **firmware location**, **firmware upgrade**, **busyout**, and **shutdown**. (See Upgrading SPE Firmware, below.)
- Troubleshooting  
Discusses the types of diagnostic tests you can perform on an SPE modem: startup test, auto-test, and back-to-back test.
- SPE Recovery  
Presents the **spe recovery** command and options, for use when an SPE port fails to connect after a certain number of consecutive attempts.
- SPE Download Maintenance  
Presents the **spe download maintenance** command and options, for use in configuring a scheduled recovery of SPEs.
- Clear an SPE  
Presents the command **clear spe**, for use in manually recovering a port that is in a suspended state.
- Upgrading SPE Firmware  
Discusses various ways to upgrade SPE firmware.

## Using Cisco Call Tracker to Manage Gateways

Cisco Call Tracker captures detailed statistics on the status and progress of active calls and retains historical data for disconnected call sessions. It collects session information such as call states and resources, traffic statistics, total bytes transmitted and received, user IP address, and disconnect reason. This data is maintained within the Call Tracker database tables, which are accessible through the Simple Network Management Protocol (SNMP), the command line interface, or syslog.

For step-by-step procedures for configuring Call Tracker and verifying configurations on the Cisco AS5300 and Cisco AS5800, refer to Call Tracker plus ISDN and AAA Enhancements for the Cisco AS5300 and Cisco AS5800 at the following URL:

[http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t3/dt\\_cltrk.htm](http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t3/dt_cltrk.htm)

## Configuring Call Tracker

To configure Call Tracker, enter **calltracker enable** command in global configuration mode.

## Verifying Call Tracker

To verify the operation of CallTracker, enter the **show call calltracker summary** command in EXEC mode.

# Managing Gatekeepers

Cisco 3640, Cisco 3660, and Cisco 7200 series platforms that are used as gatekeepers (and directory gatekeepers) employ H.323 RAS signaling to perform their function in the network hierarchy. A good discussion of this gatekeeper functionality and how to manage it can be found in Cisco High-Performance Gatekeeper at the following URL:

[http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121limit/121x/121xm/121xm\\_5/ft\\_0394.htm](http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121limit/121x/121xm/121xm_5/ft_0394.htm)

The following topics in that document are of interest with respect to managing and verifying gatekeepers in the solution.

## Configuring Load Balancing and Alternate Gatekeepers

In case a gatekeeper fails, you can assign an alternate gatekeeper to continue operation. You can create a local cluster associated with a local zone and define the alternate GK within the cluster. You will also need to configure load balancing, to determine the maximum number of calls, the percentage of CPU utilization, and the maximum percent of memory used per GK.

## Configuring Remote Clusters

You can define a group of associated GKs in a remote cluster. Simplifying management responsibilities, you can then address the cluster as you would an individual remote GK.

## Configuring Server Triggers

You can configure GKs to connect to a specific back-end server at startup, or listen to any server that wants to connect to it. This is done by configuring server triggers.

## Verifying Gatekeeper Configuration

This section provides a useful look at the results of a variety of **show gatekeeper** commands.

## Maintaining and Monitoring Gatekeeper Endpoints

This section lists a variety of **show gatekeeper** commands that are useful in monitoring and managing gatekeeper endpoints, clusters, and performance.

## Managing Modems

Modems can occasionally stop working, but reloading the firmware generally resets the modem and brings it back into service. A modem recovery feature allows the UG to identify modems that have gone out of service and automatically reloads their DSP firmware.

Modem failure and recovery are discussed in detail in the document *Configuring Modem Recovery* at the following URL:

<http://www.cisco.com/warp/public/76/modem-recovery.html>

Read the section *Modem Failure Overview* for some diagnostic tips. This section addresses the earlier MICA modems, but is applicable to NextPort modems, which use the universal port DSP.



### Note

The commands of interest to universal port cards are the **spe recovery** series. These replace the previously used **modem recovery** series. (SPE stands for Software Port Entity.) To see the series of **spe recovery** commands available from the command line, enter **spe recovery ?**. Then look for analogous commands, and their explanations, in the section *Configuring Modem Recovery*.



### Tip

Refer also to *Comparing NextPort SPE Commands to MICA Modem Commands*, at the following URL:

[http://www.cisco.com/warp/public/76/nextport\\_compare.html](http://www.cisco.com/warp/public/76/nextport_compare.html)

For the details of port management, including a command reference (applicable to both Cisco AS5350 and Cisco AS5400 platforms), refer to *Managing Port Services on the Cisco AS5400 Universal Access Server* at the following URL:

<http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t3/nextport/index.htm>

## Using and Managing MIBs

MIBs, or Management Information Bases, are databases of network performance information (the characteristics and parameters of network devices) for use by a variety of management applications. SNMP is a commonly used protocol for defining the information types in a MIB.

[Table 8-2](#) lists some useful Cisco MIBs that support the Cisco ASAP Solution.

**Table 8-2 Useful Cisco MIBs that Support the Cisco ASAP Solution**

| Dial (Modem) MIBs      | Voice MIBs                       |
|------------------------|----------------------------------|
| DIAL-CONTROL-MIB       | CISCO-VOICE-DIAL-CONTROL-MIB     |
| CISCO-DIAL-CONTROL-MIB | CISCO-CAS-IF-MIB                 |
| CISCO-POP-MGMT-MIB     | CISCO-VOICE-IF-MIB               |
| CISCO-MODEM-MGMT-MIB   | CISCO-VOICE-NUMBER-EXPANSION-MIB |
|                        | CISCO-CALL-APPLICATION-MIB       |
|                        | CISCO-SIP-UA-MIB                 |

## Obtaining MIBs

To obtain Cisco MIBs, as well as application notes related to their use, refer to Cisco MIBs at the following URL:

<http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml>

To obtain MGC MIBs, as well as application notes related to their use, refer to MGC MIBs at the following URL:

[http://cco/univercd/cc/td/doc/product/access/sc/rel9/mgc\\_mib/index.htm](http://cco/univercd/cc/td/doc/product/access/sc/rel9/mgc_mib/index.htm)

## Using MIB Locator

A convenient tool, MIB Locator, is also available that lets users browse an automated database of MIBs. A component of Cisco Feature Navigator (for which you will need a Cisco account password), MIB Locator provides a wider range of information to help the user maintain and troubleshoot networks. To use MIB Locator, follow the instructions below.

- 
- Step 1** Go to the following URL:  
<http://www.cisco.com/go/fn>
- Step 2** Enter a Cisco password as requested. The Feature Navigator window appears.
- Step 3** In the left-hand frame, click MIB Locator. The MIB Locator window appears.  
 You can search for MIBs by using the following criteria:
- Release
  - Platformfamily
  - Feature set
  - Image name
  - Specific MIB name
- Step 4** Use the criteria you want, then click the **Submit** button to issue your request.  
 You will be asked to narrow your search until you find the specific MIB you want. You can both view and download specific MIBs.

## Using MIB Objects

The values collected from CLI commands are accessible through SNMP. MIB objects are also useful for monitoring CPU utilization. (See [Checking Memory and CPU Utilization, page 8-3](#). Cisco provides the following MIB files for obtaining the equivalent output from CLI commands:

CISCO-MEMORY-POOL-MIB, OLD-CISCO-INTERFACES-MIB, and OLD-CISCO-MEMORY-MIB.

[Table 8-3](#) provides the MIB objects in the OLD-CISCO-CPU-MIB for monitoring the output of a **show processes** command.

**Table 8-3 MIB Objects in OLD-CISCO-CPU-MIB for Monitoring CPU Utilization**

| Objects  | Description                                            |
|----------|--------------------------------------------------------|
| busyPer  | CPU busy percentage in the last 5 seconds.             |
| AvgBusy1 | One-minute moving average of the CPU busy percentage.  |
| AvgBusy5 | Five-minute moving average of the CPU busy percentage. |

[Table 8-4](#) provides the MIB objects in the CISCO-MEMORY-POOL-MIB for monitoring the output of a **show memory** command.

**Table 8-4 MIB Objects in CISCO-MEMORY-POOL-MIB for Monitoring Show Memory Output**

| Objects                    | Description                                                                                        |
|----------------------------|----------------------------------------------------------------------------------------------------|
| CiscoMemoryPoolName        | A textual name assigned to the memory pool                                                         |
| CiscoMemoryPoolUsed        | Number of bytes from the memory pool that are currently in use                                     |
| CiscoMemoryPoolFree        | Indicates the number of bytes from the memory pool that are currently unused on the managed device |
| CiscoMemoryPoolLargestFree | Largest number of contiguous bytes from the memory pool that are currently unused                  |

## Cisco IOS References

The following are the most current references, and their respective URLs, for Cisco IOS commands, system error messages, and debug commands:

### Cisco IOS

For the details of Cisco IOS Release 12.2, refer to Cisco IOS Release 12.2 at the following URL:

<http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/>

## System Error Messages

The system software sends these error messages to the console (and, optionally, to a logging server on another system) during operation. Not all system error messages indicate problems with your system. Some are purely informational, and others may help diagnose problems with communications lines, internal hardware, or the system software.

Cisco IOS System Error Messages, Cisco IOS Release 12.2 at the following URL:

<http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122sup/122sems/>

## Debug Command Reference

For the details of debugging commands, refer to Cisco IOS Debug Command Reference, Cisco IOS Release 12.2 at the following URL:

<http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122sup/122debug/>







# Managing Billing and Accounting Data

---

## Introduction

Where voice services are provided, special attention must be paid to billing and accounting. This chapter supports both the Cisco ASAP Solution and the PSTN gateway solutions, and discusses how to use a variety of Cisco applications to collect billing and accounting data, as well as various parameters the service provider needs to monitor.

This chapter presents the following major topics:

- [Generating VoIP CDRs](#)
- [Collecting Billing and Accounting Data Using Cisco BAMS](#)
- [Collecting Accounting Data Using Cisco AR](#)
- [Collecting Accounting Data Using Cisco RPMS](#)

## Target Platforms

This chapter addresses the following components of the Cisco ASAP Solution and the PSTN gateway solutions: Cisco AS5000 series, Cisco BAMS. Cisco Access Registrar (AR) is also addressed. Cisco AR is used only in the Cisco ASAP Solution.

## References

For an overview of billing issues, refer to Understanding and Provisioning AAA Billing in Chapter 3, “Provisioning Shared Support Services,” in the *Cisco Wholesale Voice Solution Design and Implementation Guide* at the following URL:

[http://www.cisco.com/univercd/cc/td/doc/product/access/sc/re17/soln/wv\\_re11/wvpg/index.htm](http://www.cisco.com/univercd/cc/td/doc/product/access/sc/re17/soln/wv_re11/wvpg/index.htm)

Other references are provided as needed throughout this chapter.

## Generating VoIP CDRs

Where it is necessary to log VoIP call detail records (CDRs) for accounting or billing purposes, Cisco recommends that this be done with an external AAA (authentication, authorization, and accounting) server (either RADIUS or TACACS+). These AAA systems will commonly provide syslog-based CDR logging, postcall record processing, and a billing report-generation facility.

## Enabling Timestamps

Accurate and common timing is essential to accurate billing and accounting. If the router has no NTP synchronization, the start and stop times of each CDR will be a zero (null) value. To ensure that the H.323 start/stop records have the correct time value, Network Time Protocol (NTP) must be running on the Cisco IOS router or gateway. Two methods of enabling NTP, with or without a network time server, are shown below.

### With a Network Time Server

Use the following Cisco IOS software global config command to synchronize the Cisco IOS router or gateway to an external NTP server:

```
router#(config)# ntp server <IP address>
!--- where <IP address> is the IP address of the time server providing the clock
!--- synchronization
```

### Without a Network Timeserver

If there is no external NTP time source, the router (gateway) must be set as an NTP master clock, so it uses its internal clock as the time source. This is done with the Cisco IOS software global configuration command shown below:

```
router#(config)# ntp master
```

To ensure that the timestamps are correct, the router's clock should be set to the correct time (in privileged EXEC mode) as in the following example.

```
router# clock set 15:15:00 8 May 2001
```



#### Caution

---

On some Cisco platforms, the router clock is not backed up by a battery source, so the system time will need to be reset following a router reload or power failure.

---

## A Sample CDR Configuration

The following is a sample configuration that enables the router to generate VoIP CDRs and send them to an external syslog server.

```
router#(config)# service timestamps log datetime msec localtime
!--- Ensure that the records are timestamped with an accurate value
!
router#(config)# aaa new-model
!
router#(config)# aaa authentication login default none
```

```
!--- Enable AAA, prevent telnet authentication via AAA
router#(config)# aaa accounting connection h323 start-stop radius
!--- Generates the H.323 call start/stop CDRs
router#(config)# gw-accounting syslog
!--- Send the H.323 CDRs to the server
router#(config)# logging 10.64.6.250
!--- IP address of syslog server. Multiple syslog servers can be specified for
!--- redundancy.
```

## Collecting Billing and Accounting Data Using Cisco BAMS

A Cisco Billing and Measurements Server (BAMS) is used to collect, format, and store billing and measurements data for the Cisco MCG (Cisco SC2200 or Cisco PGW 2200 node).

The Cisco BAMS converts the Cisco MGC proprietary CDR format, known as TLV (tagged length variable), to industry-standard formats. Presently, the Cisco BAMS supports two output formats:

- Automatic message accounting billing AMA format (AMA BAF) in accordance with Telcordia specifications GR-1100 and GR-508
- An ASCII version of the AMA BAF GR-1100 call record

As the CDRs are converted, the Cisco BAMS can assign a call type to each CDR. Call types can be assigned on the basis of where the call originates and where it terminates. The relationship between origination point and termination point is determined by user-defined billing logic. If you want to use the Cisco BAMS application for accounting and billing purposes, make sure that you have read and understood the information in the *Billing and Measurements Server 2* document, at the following URL:

<http://www.cisco.com/univercd/cc/td/doc/product/access/sc/bams2/index.htm>

## Setting up Billing Logic

Cisco BAMS supports a sophisticated billing model that consists of logical zones. Using these zones, Cisco BAMS can augment each CDR with call-type information that can then be used by downstream billing systems to rate the calls.

To set up the billing logic, do the following:

- 
- Step 1** Define the zones.
  - Step 2** Establish the relationship between the zones.
  - Step 3** Define the call type for each relationship. Unique call types can be assigned on the basis of the call direction between two zones. Up to 999,999 zones can be defined.

**Note**

The above are only general steps. For the details of setting up the billing logic, refer to Chapter 3, “Configuring BAMS for BAF Billing and Measurements” and Chapter 5, “Producing BAF and ASCII Records” of the *Billing and Measurements Server 2*, at the following URL:  
<http://www.cisco.com/univercd/cc/td/doc/product/access/sc/bams2/index.htm>

---

## Using Operational Measurements

Operational measurements are generated at a predetermined, periodic interval established at system setup. The interval can be 15, 30, and 60 minutes, or 24 hours. The measurements are reported on a trunk-group basis. The operational measurement reports are written to disk in an ASCII format, and the output file can be retrieved by means of a standard FTP transfer.

### References

For a list of Cisco BAMS operational measurements that are generated for each trunk group, refer to Chapter 6, “Obtaining Measurements,” of *Billing and Measurements Server2* at the following URL:

<http://www.cisco.com/univercd/cc/td/doc/product/access/sc/bams2/index.htm>

To define or modify the Cisco BAMS operational measurements, refer to Chapter 3, “Configuring BAMS for BAF Billing and Measurements,” of *Billing and Measurements Server 2* at the above URL.

You can use Cisco VSPT to provision Cisco BAMS. For links to the appropriate documentation see Chapter 12, “Provisioning a Cisco MGC Node Using Cisco VSPT.”



#### Note

The version of Cisco VSPT will depend on your solution. Release 1.6 supports the Cisco ASAP Solution, and Release 2.1 supports the Cisco SS7 Interconnect for Voice Gateways Solution.

For more information about collecting and viewing CDRs for the Cisco SC2200 and Cisco PGW 2200, refer to the following URLs:



#### Note

The documentation you require will depend on your solution. Release 7 of the Cisco MGC software supports the Cisco ASAP Solution, and Release 9 supports the PSTN gateway solutions.

- For viewing Cisco SC2200/Cisco PGW 2200 CDRs (Cisco MGC software Release 7):  
[http://www.cisco.com/univercd/cc/td/doc/product/access/sc/rel7/omts/omts\\_ch3.htm](http://www.cisco.com/univercd/cc/td/doc/product/access/sc/rel7/omts/omts_ch3.htm)
- For viewing Cisco SC2200/Cisco PGW 2200 CDRs (Cisco MGC software Release 9):  
[http://www.cisco.com/univercd/cc/td/doc/product/access/sc/rel9/omts/omts\\_ch3.htm](http://www.cisco.com/univercd/cc/td/doc/product/access/sc/rel9/omts/omts_ch3.htm)
- For information about interfaces for retrieving Cisco SC2200/Cisco PGW 2200 CDRs (Cisco MGC software Release 7):  
<http://www.cisco.com/univercd/cc/td/doc/product/access/sc/rel7/r7billgd/r7chap1.htm>
- If you are using the Cisco BAMS to collect Cisco SC2200/Cisco PGW 2200 CDRs:  
<http://www.cisco.com/univercd/cc/td/doc/product/access/sc/bams2/index.htm>



#### Note

The Cisco PGW 2200, or PSTN Gateway 2200, is sometimes used as a term for the Cisco SC2200. The functionality of the two products is essentially the same, although they provide services for different solutions.

## Collecting Accounting Data Using Cisco AR

The Cisco Access Registrar (AR) is used as an AAA proxy-server (RADIUS or TACACS+) and collects accounting data from the Cisco AS5000 series platforms.

**Note**

Cisco AR is not used in the PSTN gateway solutions. For the Cisco ASAP Solution, the Cisco AR is the AAA server.

Cisco AR collects and stores the information contained in accounting start /stop messages. When a Cisco AS5000 series platform that uses accounting begins a session, it sends an accounting start packet describing the type of service and the user being connected to the Cisco AR server. When the session ends, the platform sends the AR server an accounting stop packet describing the type of service that was delivered. The accounting stop packet might also contain statistics such as elapsed time, input and output octets, or input and output packets. To set up and manage accounting information using the Cisco AR, see [Setting Up and Managing Accounting, page 7-14](#).

**Note**

For more information about the Cisco AR refer to the *Cisco Access Registrar* documentation at the following URL:

[http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cnsar/1\\_7/index.htm](http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cnsar/1_7/index.htm)

## Collecting Accounting Data Using Cisco RPMS

Once AAA accounting is enabled on the gateway, AAA accounting start and stop records are created for every call and are forwarded to the Cisco RPMS. You can configure Cisco RPMS to create and manage its own customer-based CDRs, as well as to forward accounting records to other AAA billing or accounting systems.

**Note**

Cisco RPMS is not used in the PSTN gateway solutions.

When configured for creating CDRs, Cisco RPMS provides additional information pertaining to pre-authentication rejection reasons (before accounting), and to policy limit information. Every customer profile has a dedicated CDR, which makes it easy to use the CDR as data for billing or other customer specific purposes.

For detailed information about how to create CDRs for accounting, read the sections Generating Call Detail Records and Defining Call Detail Records in Chapter 6, “Reporting and Accounting,” of the *Cisco Resource Policy Management Server 2.0 Configuration Guide* at the following URL:

[http://www.cisco.com/univercd/cc/td/doc/product/access/acs\\_soft/rpms/rpms\\_2-0/config/index.htm](http://www.cisco.com/univercd/cc/td/doc/product/access/acs_soft/rpms/rpms_2-0/config/index.htm)

See also [Chapter 3, “Managing Resources and Dial Services: Using Cisco RPMS.”](#)





# Upgrade Considerations

---

## Introduction

This chapter discusses general considerations that customers need to make when upgrading the Cisco ASAP Solution or the PSTN gateway solutions. Generally speaking, redundancy must be provided to support upgrades without affecting service availability.

Although it is up to the service provider to determine the service availability required by its customers, it remains good practice to ensure that voice traffic is not interrupted. In many cases, “five nines” (99.999%) availability may be required. In addition to providing redundancy to cover outages of equipment or communications channels, it is necessary to provide redundancy to support traffic during upgrades of the Cisco IOS and signaling controller software.



### Caution

---

It is the responsibility of the service provider to engineer the network in such a way as to provide the required service availability for their customers.

---

This chapter presents the following major topics:

- [Upgrading All Gateways and Gatekeepers](#)
- [Upgrading at the Billing Component Level](#)
- [Upgrading at the Network Management Level](#)

## Target Platforms

This chapter addresses the following components of the Cisco ASAP Solution and the PSTN gateway solutions: Cisco AS5000 series gateways, Cisco 3660 and Cisco 7200 series gatekeepers, Cisco MGC node components, and third-party accounting and billing platforms.

## Upgrading All Gateways and Gatekeepers

To ensure that software upgrades on a gateway (GW), gatekeepers (GK), and directory gatekeepers (DGK) in an H.323 network do not affect service availability, Cisco recommends that you provide redundancy for all components of the gatekeeper core. Note the following considerations:

- Provide multiple GWs that service the same coverage area.
- Use alternate GKs to minimize downtime during upgrades of the Cisco IOS on a GK.
- Use alternate DGKs to minimize downtime during upgrades of the Cisco IOS on a DGK.


**Note**

The most recent information about upgrading the Cisco IOS software can be found in the *Release Notes* for your software.

To upgrade software at the GW level, follow the steps below.

1. Ensure that the new Cisco IOS image is available on the TFTP server.
2. Download the new Cisco IOS files from a TFTP server to available flash memory on the selected routers beforehand. To minimize service unavailability, it is recommended that you upgrade only one router at a time.
3. Select a maintenance window that ensures the least disruption of traffic. Do the following during the maintenance window.
  - a. Redirect traffic from the routers whose software is to be upgraded.
  - b. If you have GWs that support SS7 links, you must take those links out of service (OOS) on the Cisco SC2200 that supports those links.
  - c. Reboot the routers to move the new image from flash memory to RAM. This activates the IOS upgrade.


**Note**

Rebooting can take up to 5 minutes.

## Upgrading at the Billing Component Level

It is essential that billing information not be lost. In addition to providing redundancy to cover outages of equipment or communications channels, it is necessary to provide redundancy to maintain billing data during upgrades of software to support billing applications. Components to consider include AAA/RADIUS servers, OSP (Open Systems Protocol) servers, and other servers providing third-party billing and settlement applications.

## Upgrading at the Network Management Level

It is generally not necessary to provide redundancy at the network management level, because these applications can go out of service during a maintenance window with minimal impact on traffic. However, it is the responsibility of the service provider to consider any possible effects such outages may have, and provide redundancy if necessary.



## Upgrading the Cisco ASAP Solution

For information about upgrading the Cisco ASAP Solution, refer to the following documents:

- *Cisco ASAP Solution Release Notes* at the following URL:  
<http://www.cisco.com/univercd/cc/td/doc/product/access/solution/asap/index.htm>
- Chapter 1, “Solution-Level Upgrade Procedures,” of the *Cisco SS7 Interconnect for Access Servers and Voice Gateways Upgrade Guide*  
<http://www.cisco.com/univercd/cc/td/doc/product/access/sc/re17/soln/das/upgrade/index.htm>

## Upgrading Cisco SS7 Interconnect for Voice Gateways Solution

For information about upgrading the Cisco SS7 Interconnect for Voice Gateways Solution, refer to the *Cisco SS7 Interconnect for Access Servers and Voice Gateways Upgrade*, Release 2.x at the following URL:

<http://www.cisco.com/univercd/cc/td/doc/product/access/sc/re19/soln/voip20/upgrade/index.htm>

## Upgrading the Cisco PSTN Gateway Solution

For information about upgrading the Cisco PSTN Gateway Solution, refer to the following documents:

- *Cisco PSTN Gateway Solution Release Notes* at the following URL:  
<http://cco/univercd/cc/td/doc/solution/dialvoic/pstngw/relnote/index.htm>





# Operating and Maintaining SS7 Components

## Introduction

This chapter presents references to a variety of operations and maintenance practices specific to networks that support SS7 interconnect (optional in the Cisco ASAP Solution, required in the PSTN gateway solutions). The entity managed is the Cisco media gateway controller (MGC) node, which includes the host platforms and Cisco Signaling Link Terminals (SLTs). The Cisco MGC itself is a Sun Netra UNIX host running Cisco MGC software Release 7 or Cisco MGC software Release 9.

Tips for troubleshooting SS7 components and links are provided in [Chapter 13, “Troubleshooting SS7 Interconnect Problems: Cisco MGC Node.”](#)



### Note

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

To provision MGC node components using the Cisco Voice Services Provisioning Tool (VSPT), see [Chapter 12, “Provisioning a Cisco MGC Node Using Cisco VSPT.”](#)

## Target Platforms

The tasks in this chapter address the following components of the Cisco ASAP Solution and the PSTN gateway solutions: components of the Cisco MGC node.

## References

There are different versions of the Cisco MGC software operations, maintenance, and troubleshooting guide. Release 7 applies to the Cisco ASAP Solution, and Release 9 applies to the PSTN gateway solutions.

### Cisco MGC Release 7

The master reference is the *Cisco MGC Software Release 7 Operations, Maintenance, and Troubleshooting Guide* at the following URL:

<http://www.cisco.com/univercd/cc/td/doc/product/access/sc/re17/omts/index.htm>

## Cisco MGC Release 9

The master reference is the *Cisco MGC Software Release 9 Operations, Maintenance, and Troubleshooting Guide* at the following URL:

<http://www.cisco.com/univercd/cc/td/doc/product/access/sc/re19/omts/index.htm>

This chapter directs you to high-level operations and maintenance procedures in both documents. Make sure you are familiar with the above guides, including their prefaces and introductions.

## Operations and Maintenance Tasks

The major operations and maintenance tasks in the above-referenced guides are summarized in [Table 11-1](#)

**Table 11-1 Major Sections of the Cisco MGC Software Release 7 and Release 9 Operations, Maintenance, and Troubleshooting Guides**

| Chapter/<br>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 disk monitor program, and backup procedures.                     |
| 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.                                             |

Although the troubleshooting chapters and appendixes in the above document are also useful, see [Chapter 13, “Troubleshooting SS7 Interconnect Problems: Cisco MGC Node”](#) for a summary overview of key tasks. The following high-level task categories are covered there:

- [Using System Output](#)
- [Resolving SS7 Network Problems](#)
- [Resolving Bearer Channel Connection Problems](#)
- [Tracing](#)
- [Troubleshooting the Cisco MGC Platform](#)





# Provisioning a Cisco MGC Node Using Cisco VSPT

---

## Introduction

This chapter provides references for how to use the Cisco Voice Services Provisioning Tool (VSPT), Release 1.6 and Release 2.2, to provision Cisco Media Gateway Controller (MGC) nodes, such as a Cisco SC2200 Signaling Controller, to support SS7 signaling.

VSPT Release 1.6 supports the following solutions:

- Cisco ASAP Solution
- Release 1.3 of the Cisco SS7 Interconnect for Voice Gateways Solution

VSPT Release 2.2 supports

- Cisco PSTN Gateway Solution
- Release 2.0 of the Cisco SS7 Interconnect for Voice Gateways Solution.

The Cisco VSPT provides a GUI for the creation, modification, and execution of signaling connections, trunk groups, trunks, routes, and dial plans. It also allows users to import existing configurations for modification and then download the modified configurations to the same or different devices. To simplify operator tasks, such as trunk group provisioning, Cisco VSPT employs a series of wizard-style templates combined with a user interface tailored for provisioning. Cisco VSPT automatically generates the Man Machine Language (MML) or command-line interface (CLI) scripts used to configure the network elements.



### Note

---

The Cisco PGW 2200 configured for signaling is also referred to in a variety of documents as the Cisco SC2200, the earlier term.

---

## Target Platforms

The tasks in this chapter address the following components of the Cisco ASAP Solution and the PSTN gateway solutions: components of the Cisco MGC node.

## References

References are provided for the following topics:

- [Using Cisco VSPT](#)
- [Using MML](#)

## Using Cisco VSPT

### Release 1.6

For more information about how to use Cisco VSPT to provision a Cisco MGC node for the Cisco ASAP Solution, including Cisco BAMS and Cisco SC2200, refer to the *Cisco Voice Services Provisioning Tool User's Guide, Version 1.6* at the following URL:

<http://www.cisco.com/univercd/cc/td/doc/product/access/sc/rel7/dart16/index.htm>

The following are additional documentation about Cisco VSPT used in provisioning Cisco MGC nodes in voice and dial solutions:

- Chapter 3, “Provisioning the Cisco SS7 Interconnect for Voice Gateways Solution by Using VSPT,” of the *Cisco SS7 Interconnect for Voice Gateways Version 1.3 Provisioning Guide* at the following URL:

<http://www.cisco.com/univercd/cc/td/doc/product/access/sc/rel7/soln/voip13/provgde/>

- Chapter 4, “Provisioning Dial Plans with VSPT,” of the *Cisco MGC Software Release 7 Dial Plan Guide* at the following URL:

<http://www.cisco.com/univercd/cc/td/doc/product/access/sc/rel7/dplan/>

### Release 2.2

For more information about how to use Cisco VSPT to provision a Cisco MGC node for the Cisco SS7 Interconnect for Voice Gateways 2.0 Solution, including Cisco BAMS and Cisco PGW 2200, refer to the *Cisco Voice Services Provisioning Tool User's Guide, Version 2.2* at the following URL:

<http://www.cisco.com/univercd/cc/td/doc/product/access/sc/rel9/vspt22/index.htm>

## Using MML

For information about using MML in Release 7.4(x) of the Cisco MGC software, refer to the *Cisco Media Gateway Controller Software Release 7 MML Command Guide* at the following URL:

<http://www.cisco.com/univercd/cc/td/doc/product/access/sc/rel7/r7mmlref/index.htm>

For information about using MML in Release 9.x of the Cisco MGC software, refer to the *Cisco Media Gateway Controller Software Release 7 MML Command Guide* at the following URL:

<http://www.cisco.com/univercd/cc/td/doc/product/access/sc/rel9/mmlref/index.htm>





# Troubleshooting SS7 Interconnect Problems: Cisco MGC Node

---

## Introduction

This chapter presents SS7 interconnect troubleshooting tasks related to the Cisco ASAP Solution and the PSTN gateway solutions that are performed on elements of the Cisco Media Gateway Controller (MGC) node. The components of these solutions are discussed in [Chapter 11, “Operating and Maintaining SS7 Components.”](#)

The Cisco MGC node is made up of Cisco MGC host(s) and Cisco Signaling Link Terminals (SLTs) connected by a LAN switch. The Cisco MGC Node is used in two products: the Cisco SC2200 and the Cisco PGW 2200.



### Note

---

The procedures in this chapter *apply only* to Cisco ASAP Solutions that use SS7 interconnect or Cisco SS7 Interconnect for Voice Gateways Solutions.

---

This chapter presents the following major troubleshooting topics:

- [Using System Output](#)
- [Resolving SS7 Network Problems](#)
- [Resolving Bearer Channel Connection Problems](#)
- [Tracing](#)
- [Troubleshooting the Cisco MGC Platform](#)



### Tip

---

See also [Task Summary, page 13-2](#).

---

## Target Platforms

The tasks in this chapter address the following components of the Cisco ASAP Solution and the PSTN gateway solutions: components of the Cisco MGC node.

## References

The Cisco ASAP Solution and Release 1.3 of the Cisco SS7 Interconnect for Voice Gateways uses Release 7 of the Cisco MGC software; Cisco PSTN Gateway Solution and Release 2.0 of the Cisco SS7 Interconnect for Voice Gateways Solution uses Release 9 of the Cisco MGC software. Some documentation such as the following can be used in both releases:

- For information on Cisco MGC node alarms and logs for Release 7, refer to *Cisco Media Gateway Controller Software Release 7 Messages Reference Guide* at the following URL:  
<http://www.cisco.com/univercd/cc/td/doc/product/access/sc/rel7/r7msgref/>
- For information on Cisco MGC dial plans for Release 7, refer to *Cisco Media Gateway Controller Software Release 7 Dial Plan Guide* at the following URL:  
<http://www.cisco.com/univercd/cc/td/doc/product/access/sc/rel7/dplan/>
- For information on Cisco MGC node alarms and logs for Release 9, refer to *Cisco Media Gateway Controller Software Release 9 Messages Reference Guide* at the following URL:  
<http://www.cisco.com/univercd/cc/td/doc/product/access/sc/rel9/errmsg/>
- For information on Cisco MGC dial plans for Release 9, refer to *Cisco Media Gateway Controller Software Release 9 Dial Plan Guide* at the following URL:  
<http://www.cisco.com/univercd/cc/td/doc/product/access/sc/rel9/dplan/>

The respective references are provided below.

### Cisco MGC Release 7

For the following procedures, refer to *Cisco Media Gateway Controller Software Release 7 Operations, Maintenance, and Troubleshooting Guide* at the following URL:

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

### Cisco MGC Release 9

For the following procedures, refer to *Cisco Media Gateway Controller Software Release 9 Operations, Maintenance, and Troubleshooting Guide* at the following URL:

<http://www.cisco.com/univercd/cc/td/doc/product/access/sc/rel9/omts/>

## Task Summary

The tasks in this chapter are listed below, grouped by major category.

### Using System Output

- [Retrieving All Active Alarms](#)
- [Viewing System Logs](#)
- [Using Alarm Troubleshooting Procedures](#)

## Resolving SS7 Network Problems

- Restoring an SS7 Link to Service
- Resolving an SS7 Load Sharing Malfunction
- Resolving Physical Layer Failures
- Correcting Bouncing SS7 Links
- Restoring an SS7 DPC to Service
- Restoring an SS7 Route to Service
- Restoring an Unavailable SS7 DPC
- Verifying MTP Timer Settings
- Modifying MTP Timer Settings
- Verifying the Proper Loading of a Dial Plan

## Resolving Bearer Channel Connection Problems

- Querying Local and Remote CIC States
- Performing CIC Validation Tests
- Resolving ISDN D-Channel Discrepancies
- Unblocking CICs
- Resetting CICs
- Resolving Stuck CICs
- Running a Manual Continuity Test
- Verifying Continuity Test Settings
- Restoring a Media Gateway IP Destination/Link to Service
- Calls Fail at the Cisco MGC
- Modifying Redundant Link Manager Timers

## Tracing

- Performing a Call Trace
- Alternatives to Call Tracing
- Performing a TCAP Trace

## Troubleshooting the Cisco MGC Platform

- Deleting Unnecessary Files
- Recovering from a Switchover Failure
- Recovering from Cisco MGC Host(s) Failure
- Restoring Stored Configuration Data
- Verifying Proper Configuration of Replication

- [Measurements Are Not Being Generated](#)
- [Call Detail Records Are Not Being Generated](#)
- [Rebooting Your System to Modify Properties](#)
- [Resolving a Failed Connection to a Peer](#)

# Retrieving All Active Alarms

## Description

|                           |                                                                                                         |
|---------------------------|---------------------------------------------------------------------------------------------------------|
| <b>Summary</b>            | You must retrieve all of the active alarms on the Cisco MGC node to identify SS7 interconnect problems. |
| <b>Target Platform(s)</b> | Cisco MGC (Cisco SC2200 or Cisco PGW 2200) and Cisco SLT (Cisco 2611 or Cisco 2651)                     |
| <b>Application</b>        | See <a href="#">Introduction, page 13-1</a>                                                             |
| <b>Frequency</b>          | As needed                                                                                               |

## Reference

Depends on the solution and related release of the Cisco MGC software. See [References, page 13-2](#).

## Procedure

To retrieve all active alarms:

- 
- Step 1** In the above reference, refer to Chapter 8, “Troubleshooting the Cisco MGC Node.”
  - Step 2** Read the section Retrieving All Active Alarms.
  - Step 3** As appropriate, follow the steps in one or more of the following sections:
    - a. Acknowledging Alarms
    - b. Clearing Alarms
-

# Viewing System Logs

## Description

|                           |                                                                                         |
|---------------------------|-----------------------------------------------------------------------------------------|
| <b>Summary</b>            | Viewing Cisco MGC system logs can provide additional information about system problems. |
| <b>Target Platform(s)</b> | Cisco MGC (Cisco SC2200 or Cisco PGW 2200)                                              |
| <b>Application</b>        | See <a href="#">Introduction, page 13-1</a>                                             |
| <b>Frequency</b>          | As needed                                                                               |

## Reference

Depends on the solution and related release of the Cisco MGC software. See [References, page 13-2](#).

## Procedure

To view system logs:

- 
- Step 1** In the above reference, refer to Chapter 3, “Cisco MGC Node Operations.”
  - Step 2** Read the section Using the Log Viewer and follow the instructions therein.
  - Step 3** Also refer to Chapter 8, “Troubleshooting the Cisco MGC Node,” and follow the instructions in the section Viewing System Logs.
-

# Using Alarm Troubleshooting Procedures

## Description

|                           |                                                                                                           |
|---------------------------|-----------------------------------------------------------------------------------------------------------|
| <b>Summary</b>            | Some Cisco MGC node alarms require that the user take corrective action to resolve the indicated problem. |
| <b>Target Platform(s)</b> | Cisco MGC (Cisco SC2200 or Cisco PGW 2200) and Cisco SLT (Cisco 2611 or Cisco 2651)                       |
| <b>Application</b>        | See <a href="#">Introduction, page 13-1</a>                                                               |
| <b>Frequency</b>          | As needed                                                                                                 |

## Reference

Depends on the solution and related release of the Cisco MGC software. See [References, page 13-2](#).

## Procedure

To retrieve all active alarms:

- 
- Step 1** In the above reference, refer to Chapter 8, “Troubleshooting the Cisco MGC Node.”
  - Step 2** Search for the alarm of interest in the Alarm Troubleshooting Procedures section.
  - Step 3** Perform the steps listed in the appropriate section.

If the alarm is not listed in the Alarm Troubleshooting Procedures section, refer to the *Cisco Media Gateway Controller Software Release 7 System Messages Guide* for information on the alarm. See [References, page 13-2](#).

---

## Notes

- *Related documents: Cisco Media Gateway Controller Software Release 7 System Messages Guide*

# Restoring an SS7 Link to Service

## Description

|                           |                                                         |
|---------------------------|---------------------------------------------------------|
| <b>Summary</b>            | Use this procedure to resolve SS7 link problems.        |
| <b>Target Platform(s)</b> | Cisco MGC (Cisco SC2200 or Cisco PGW 2200) or Cisco SLT |
| <b>Application</b>        | See <a href="#">Introduction, page 13-1</a>             |
| <b>Frequency</b>          | As needed                                               |

## Reference

Depends on the solution and related release of the Cisco MGC software. See [References, page 13-2](#).

## Procedure

To restore an SS7 link to service:

- 
- |               |                                                                                   |
|---------------|-----------------------------------------------------------------------------------|
| <b>Step 1</b> | In the above reference, refer to Chapter 8, “Troubleshooting the Cisco MGC Node.” |
| <b>Step 2</b> | Read the section SS7 Link is Out of Service and follow the instructions therein.  |
-



# Resolving an SS7 Load Sharing Malfunction

## Description

|                           |                                                          |
|---------------------------|----------------------------------------------------------|
| <b>Summary</b>            | Use this procedure to resolve SS7 load sharing problems. |
| <b>Target Platform(s)</b> | Cisco MGC (Cisco SC2200 or Cisco PGW 2200)               |
| <b>Application</b>        | See <a href="#">Introduction, page 13-1</a>              |
| <b>Frequency</b>          | As needed                                                |

## Reference

Depends on the solution and related release of the Cisco MGC software. See [References, page 13-2](#).

## Procedure

To resolve an SS7 load sharing malfunction:

- 
- |               |                                                                                    |
|---------------|------------------------------------------------------------------------------------|
| <b>Step 1</b> | In the above reference, refer to Chapter 8, “Troubleshooting the Cisco MGC Node.”  |
| <b>Step 2</b> | Read the section SS7 Load Sharing Malfunction and follow the instructions therein. |
-

# Resolving Physical Layer Failures

## Description

|                           |                                                                              |
|---------------------------|------------------------------------------------------------------------------|
| <b>Summary</b>            | Use this procedure to resolve physical layer problems in the Cisco MGC node. |
| <b>Target Platform(s)</b> | Cisco MGC (Cisco SC2200 or Cisco PGW 2200) or Cisco SLT                      |
| <b>Application</b>        | See <a href="#">Introduction, page 13-1</a>                                  |
| <b>Frequency</b>          | As needed                                                                    |

## Reference

Depends on the solution and related release of the Cisco MGC software. See [References, page 13-2](#).

## Procedure

To resolve physical layer problems in the Cisco MGC node:

- 
- |               |                                                                                   |
|---------------|-----------------------------------------------------------------------------------|
| <b>Step 1</b> | In the above reference, refer to Chapter 8, “Troubleshooting the Cisco MGC Node.” |
| <b>Step 2</b> | Read the section Physical Layer Failure and follow the instructions therein.      |
-

# Correcting Bouncing SS7 Links

## Description

|                           |                                                                                                                      |
|---------------------------|----------------------------------------------------------------------------------------------------------------------|
| <b>Summary</b>            | Use this procedure to correct a situation where SS7 links are “bouncing,” or going in and out of service repeatedly. |
| <b>Target Platform(s)</b> | Cisco MGC (Cisco SC2200 or Cisco PGW 2200) or Cisco SLT                                                              |
| <b>Application</b>        | See <a href="#">Introduction, page 13-1</a>                                                                          |
| <b>Frequency</b>          | As needed                                                                                                            |

## Reference

Depends on the solution and related release of the Cisco MGC software. See [References, page 13-2](#).

## Procedure

To correct bouncing SS7 links:

- 
- |               |                                                                                   |
|---------------|-----------------------------------------------------------------------------------|
| <b>Step 1</b> | In the above reference, refer to Chapter 8, “Troubleshooting the Cisco MGC Node.” |
| <b>Step 2</b> | Read the section Bouncing SS7 Links and follow the instructions therein.          |
-

# Restoring an SS7 DPC to Service

## Description

|                           |                                                                               |
|---------------------------|-------------------------------------------------------------------------------|
| <b>Summary</b>            | Use this procedure to restore an SS7 DPC (destination point code) to service. |
| <b>Target Platform(s)</b> | Cisco MGC (Cisco SC2200 or Cisco PGW 2200)                                    |
| <b>Application</b>        | See <a href="#">Introduction, page 13-1</a>                                   |
| <b>Frequency</b>          | As needed                                                                     |

## Reference

Depends on the solution and related release of the Cisco MGC software. See [References, page 13-2](#).

## Procedure

To restore an SS7 destination to service:

- 
- |               |                                                                                         |
|---------------|-----------------------------------------------------------------------------------------|
| <b>Step 1</b> | In the above reference, refer to Chapter 8, “Troubleshooting the Cisco MGC Node.”       |
| <b>Step 2</b> | Read the section SS7 Destination is Out-of-Service and follow the instructions therein. |
-

# Restoring an SS7 Route to Service

## Description

|                           |                                                         |
|---------------------------|---------------------------------------------------------|
| <b>Summary</b>            | Use this procedure to restore an SS7 route to service.  |
| <b>Target Platform(s)</b> | Cisco MGC (Cisco SC2200 or Cisco PGW 2200) or Cisco SLT |
| <b>Application</b>        | See <a href="#">Introduction, page 13-1</a>             |
| <b>Frequency</b>          | As needed                                               |

## Reference

Depends on the solution and related release of the Cisco MGC software. See [References, page 13-2](#).

## Procedure

To restore an SS7 route to service:

- 
- |               |                                                                                   |
|---------------|-----------------------------------------------------------------------------------|
| <b>Step 1</b> | In the above reference, refer to Chapter 8, “Troubleshooting the Cisco MGC Node.” |
| <b>Step 2</b> | Read the section SS7 Route is Out-of-Service and follow the instructions therein. |
-

# Restoring an Unavailable SS7 DPC

## Description

|                           |                                                                                                                                                                    |
|---------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Summary</b>            | Use this procedure to correct a situation where an SS7 DPC is unavailable. An SS7 DPC is unavailable when all of the routes to the destination are out-of-service. |
| <b>Target Platform(s)</b> | Cisco MGC (Cisco SC2200 or Cisco PGW 2200) or Cisco SLT                                                                                                            |
| <b>Application</b>        | See <a href="#">Introduction, page 13-1</a>                                                                                                                        |
| <b>Frequency</b>          | As needed                                                                                                                                                          |

## Reference

Depends on the solution and related release of the Cisco MGC software. See [References, page 13-2](#).

## Procedure

To make an SS7 DPC available:

- 
- |               |                                                                                      |
|---------------|--------------------------------------------------------------------------------------|
| <b>Step 1</b> | In the above reference, refer to Chapter 8, “Troubleshooting the Cisco MGC Node.”    |
| <b>Step 2</b> | Read the section SS7 Destination is Unavailable and follow the instructions therein. |
- 

## Notes

- *Related tasks:* [Restoring an SS7 Route to Service, page 13-13](#)

# Verifying MTP Timer Settings

## Description

|                           |                                                                                                                                                                           |
|---------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Summary</b>            | Troubleshooting SS7 network problems sometimes requires that you verify that your local message transfer part (MTP) timer settings match those being used on the far end. |
| <b>Target Platform(s)</b> | Cisco MGC (Cisco SC2200 or Cisco PGW 2200) or Cisco SLT                                                                                                                   |
| <b>Application</b>        | See <a href="#">Introduction, page 13-1</a>                                                                                                                               |
| <b>Frequency</b>          | As needed                                                                                                                                                                 |

## Reference

Depends on the solution and related release of the Cisco MGC software. See [References, page 13-2](#).

## Procedure

To verify the settings of your local MTP timers:

- 
- |               |                                                                                                        |
|---------------|--------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | In the above reference, refer to Chapter 8, “Troubleshooting the Cisco MGC Node.”                      |
| <b>Step 2</b> | Read the section Verifying MTP Timer Settings.                                                         |
| <b>Step 3</b> | If necessary, modify your MTP timer settings as described in the Modifying MTP Timer Settings section. |
- 

## Notes

- *Related tasks:* [Modifying MTP Timer Settings, page 13-16](#)

# Modifying MTP Timer Settings

## Description

|                           |                                                                     |
|---------------------------|---------------------------------------------------------------------|
| <b>Summary</b>            | Use this procedure to modify the settings of your local MTP timers. |
| <b>Target Platform(s)</b> | Cisco MGC (Cisco SC2200 or Cisco PGW 2200) or Cisco SLT             |
| <b>Application</b>        | See <a href="#">Introduction, page 13-1</a>                         |
| <b>Frequency</b>          | As needed                                                           |

## Reference

Depends on the solution and related release of the Cisco MGC software. See [References, page 13-2](#).

## Procedure

To modify the settings of the MTP timers:

- 
- |               |                                                                                    |
|---------------|------------------------------------------------------------------------------------|
| <b>Step 1</b> | In the above reference, refer to Chapter 8, “Troubleshooting the Cisco MGC Node.”  |
| <b>Step 2</b> | Read the section Modifying MTP Timer Settings and follow the instructions therein. |
- 

## Notes

- *Related tasks:* [Verifying MTP Timer Settings, page 13-15](#), and [Rebooting Your System to Modify Properties, page 13-40](#)



# Verifying the Proper Loading of a Dial Plan

## Description

|                           |                                                                    |
|---------------------------|--------------------------------------------------------------------|
| <b>Summary</b>            | Use this procedure to verify that a dial plan has loaded properly. |
| <b>Target Platform(s)</b> | Cisco MGC (Cisco SC2200 or Cisco PGW 2200)                         |
| <b>Application</b>        | See <a href="#">Introduction, page 13-1</a>                        |
| <b>Frequency</b>          | As needed                                                          |

## Reference

Depends on the solution and related release of the Cisco MGC software. See [References, page 13-2](#).

## Procedure

To verify that a dial plan has loaded properly:

- 
- |               |                                                                                               |
|---------------|-----------------------------------------------------------------------------------------------|
| <b>Step 1</b> | In the above reference, refer to Chapter 8, “Troubleshooting the Cisco MGC Node.”             |
| <b>Step 2</b> | Read the section Verifying Proper Loading of a Dial Plan and follow the instructions therein. |
- 

## Notes

- *Related documents:*
  - *Cisco Media Gateway Controller Software Release 7 Dial Plan Guide*
  - *Cisco Media Gateway Controller Software Release 9 Dial Plan Guide*

# Querying Local and Remote CIC States

## Description

|                           |                                                                                                                                                                                                                                                                           |
|---------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Summary</b>            | In the course of troubleshooting problems with your bearer channels, you may need to query the local and remote states of the related circuit identification codes (CICs), to verify that they match. This procedure contains steps to query local and remote CIC states. |
| <b>Target Platform(s)</b> | Cisco MGC (Cisco SC2200 or Cisco PGW 2200)                                                                                                                                                                                                                                |
| <b>Application</b>        | See <a href="#">Introduction, page 13-1</a>                                                                                                                                                                                                                               |
| <b>Frequency</b>          | As needed                                                                                                                                                                                                                                                                 |

## Reference

Depends on the solution and related release of the Cisco MGC software. See [References, page 13-2](#).

## Procedure

To query the state of a local or remote CIC:

- 
- |               |                                                                                                                                                                      |
|---------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | In the above reference, refer to Chapter 8, “Troubleshooting the Cisco MGC Node.”                                                                                    |
| <b>Step 2</b> | Read the section Querying Local and Remote CIC States.                                                                                                               |
| <b>Step 3</b> | If the local and remote CIC states do not match, attempt to resolve the state mismatch using the steps in the Resolving Local and Remote CIC State Mismatch section. |
- 

## Notes

- *Related tasks:* [Resolving Local and Remote CIC State Mismatch, page 13-19](#)

# Resolving Local and Remote CIC State Mismatch

## Description

|                           |                                                                                                                                                                         |
|---------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Summary</b>            | 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 by using this procedure. |
| <b>Target Platform(s)</b> | Cisco MGC (Cisco SC2200 or Cisco PGW 2200)                                                                                                                              |
| <b>Application</b>        | See <a href="#">Introduction, page 13-1</a>                                                                                                                             |
| <b>Frequency</b>          | As needed                                                                                                                                                               |

## Reference

Depends on the solution and related release of the Cisco MGC software. See [References, page 13-2](#).

## Procedure

To resolve a state mismatch between the local and remote CICs:

- 
- |               |                                                                                                     |
|---------------|-----------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | In the above reference, refer to Chapter 8, “Troubleshooting the Cisco MGC Node.”                   |
| <b>Step 2</b> | Read the section Resolving Local and Remote CIC State Mismatch and follow the instructions therein. |
- 

## Notes

- *Related tasks:* [Querying Local and Remote CIC States, page 13-18](#)

# Performing CIC Validation Tests

## Description

|                           |                                                                                                                                                                                                                                                                                                                  |
|---------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Summary</b>            | When performing initial turn-up of CICs or in troubleshooting certain problems with your bearer channels, you may want to perform a CIC 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. |
| <b>Target Platform(s)</b> | Cisco MGC (Cisco SC2200 or Cisco PGW 2200)                                                                                                                                                                                                                                                                       |
| <b>Application</b>        | See <a href="#">Introduction, page 13-1</a>                                                                                                                                                                                                                                                                      |
| <b>Frequency</b>          | As needed                                                                                                                                                                                                                                                                                                        |

## Reference

Depends on the solution and related release of the Cisco MGC software. See [References, page 13-2](#).

## Procedure

To perform a CIC validation test:

- 
- Step 1** In the above reference, refer to Chapter 8, “Troubleshooting the Cisco MGC Node.”
  - Step 2** Read the section Performing a CIC Validation Test and follow the instructions therein.
-

# Resolving ISDN D-Channel Discrepancies

## Description

|                           |                                                                                                                                                                                                                     |
|---------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Summary</b>            | 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, use this procedure. |
| <b>Target Platform(s)</b> | Cisco MGC (Cisco SC2200 or Cisco PGW 2200) and Cisco AS5000 series                                                                                                                                                  |
| <b>Application</b>        | See <a href="#">Introduction, page 13-1</a>                                                                                                                                                                         |
| <b>Frequency</b>          | As needed                                                                                                                                                                                                           |

## Reference

Depends on the solution and related release of the Cisco MGC software. See [References, page 13-2](#).

## Procedure

To resolve ISDN D-channel discrepancies:

- 
- |               |                                                                                              |
|---------------|----------------------------------------------------------------------------------------------|
| <b>Step 1</b> | In the above reference, refer to Chapter 8, “Troubleshooting the Cisco MGC Node.”            |
| <b>Step 2</b> | Read the section Resolving ISDN D-Channel Discrepancies and follow the instructions therein. |
-

# Unblocking CICs

## Description

|                           |                                             |
|---------------------------|---------------------------------------------|
| <b>Summary</b>            | Contains steps for unblocking CICs.         |
| <b>Target Platform(s)</b> | Cisco MGC (Cisco SC2200 or Cisco PGW 2200)  |
| <b>Application</b>        | See <a href="#">Introduction, page 13-1</a> |
| <b>Frequency</b>          | As needed                                   |

## Reference

Depends on the solution and related release of the Cisco MGC software. See [References, page 13-2](#).

## Procedure

To unblock CICs:

- 
- |               |                                                                                   |
|---------------|-----------------------------------------------------------------------------------|
| <b>Step 1</b> | In the above reference, refer to Chapter 8, “Troubleshooting the Cisco MGC Node.” |
| <b>Step 2</b> | Read the section Unblocking CICs and follow the instructions therein.             |
| <b>Step 3</b> | If the CICs are still blocked, perform the steps in the Resetting CICs section.   |
- 

## Notes

- *Related tasks:* [Resetting CICs, page 13-23](#)

# Resetting CICs

## Description

|                           |                                             |
|---------------------------|---------------------------------------------|
| <b>Summary</b>            | Use this procedure to reset CICs.           |
| <b>Target Platform(s)</b> | Cisco MGC (Cisco SC2200 or Cisco PGW 2200)  |
| <b>Application</b>        | See <a href="#">Introduction, page 13-1</a> |
| <b>Frequency</b>          | As needed                                   |

## Reference

Depends on the solution and related release of the Cisco MGC software. See [References, page 13-2](#).

## Procedure

To reset CICs:

- 
- |               |                                                                                            |
|---------------|--------------------------------------------------------------------------------------------|
| <b>Step 1</b> | In the above reference, refer to Chapter 8, “Troubleshooting the Cisco MGC Node.”          |
| <b>Step 2</b> | Read the section Resetting CICs and follow the instructions therein.                       |
| <b>Step 3</b> | If the CICs did not reset properly, perform the steps in the Resolving Stuck CICs section. |
- 

## Notes

- *Related tasks:* [Resolving Stuck CICs, page 13-24](#)

# Resolving Stuck CICs

## Description

**Summary** A stuck or hung CIC occurs when one or more bearer channels associated with a single call instance refuses to return to the idle call state, despite attempts to clear it manually. 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 the timeslot) on the media gateway.

Stuck CICs are typically resolved automatically. This procedure is a manual method of resolving stuck CICs.

**Target Platform(s)** Cisco MGC (Cisco SC2200 or Cisco PGW 2200) and Cisco AS5000 series

**Application** See [Introduction, page 13-1](#)

**Frequency** As needed

## Reference

Depends on the solution and related release of the Cisco MGC software. See [References, page 13-2](#).

## Procedure

To resolve a state mismatch between the local and remote CICs:

- 
- Step 1** In the above reference, refer to Chapter 8, "Troubleshooting the Cisco MGC Node."
  - Step 2** Read the section Resolving Stuck CICs and follow the instructions therein.
-



# Running a Manual Continuity Test

## Description

|                           |                                                                 |
|---------------------------|-----------------------------------------------------------------|
| <b>Summary</b>            | Use this procedure to perform a continuity test (COT) manually. |
| <b>Target Platform(s)</b> | Cisco MGC (Cisco SC2200 or Cisco PGW 2200)                      |
| <b>Application</b>        | See <a href="#">Introduction, page 13-1</a>                     |
| <b>Frequency</b>          | As needed                                                       |

## Reference

Depends on the solution and related release of the Cisco MGC software. See [References, page 13-2](#).

## Procedure

To run a manual COT:

- 
- |               |                                                                                        |
|---------------|----------------------------------------------------------------------------------------|
| <b>Step 1</b> | In the above reference, refer to Chapter 8, “Troubleshooting the Cisco MGC Node.”      |
| <b>Step 2</b> | Read the section Running a Manual Continuity Test and follow the instructions therein. |
| <b>Step 3</b> | If the COT fails, perform the steps in the Verifying Continuity Test Settings section. |
- 

## Notes

- *Related tasks:* [Verifying Continuity Test Settings, page 13-26](#)

# Verifying Continuity Test Settings

## Description

|                           |                                                                                        |
|---------------------------|----------------------------------------------------------------------------------------|
| <b>Summary</b>            | If a COT should fail, use this procedure to verify that your COT settings are correct. |
| <b>Target Platform(s)</b> | Cisco MGC (Cisco SC2200 or Cisco PGW 2200) and Cisco AS5000 series                     |
| <b>Application</b>        | See <a href="#">Introduction, page 13-1</a>                                            |
| <b>Frequency</b>          | As needed                                                                              |

## Reference

Depends on the solution and related release of the Cisco MGC software. See [References, page 13-2](#).

## Procedure

To verify the COT settings:

- 
- |               |                                                                                          |
|---------------|------------------------------------------------------------------------------------------|
| <b>Step 1</b> | In the above reference, refer to Chapter 8, “Troubleshooting the Cisco MGC Node.”        |
| <b>Step 2</b> | Read the section Verifying Continuity Test Settings and follow the instructions therein. |
- 

## Notes

- *Related tasks:* [Running a Manual Continuity Test, page 13-25](#)

# Restoring a Media Gateway IP Destination/Link to Service

## Description

|                           |                                                                                                                               |
|---------------------------|-------------------------------------------------------------------------------------------------------------------------------|
| <b>Summary</b>            | Use this procedure to restore service to an IP link or destination associated with a media gateway.                           |
| <b>Note</b>               | An IP destination to a media gateway is out-of-service when both IP links associated with the destination are out-of-service. |
| <b>Target Platform(s)</b> | Cisco MGC (Cisco SC2200 or Cisco PGW 2200) and Cisco AS5000 series                                                            |
| <b>Application</b>        | See <a href="#">Introduction, page 13-1</a>                                                                                   |
| <b>Frequency</b>          | As needed                                                                                                                     |

## Reference

Depends on the solution and related release of the Cisco MGC software. See [References, page 13-2](#).

## Procedure

To restore service to an IP link or destination associated with a media gateway:

- 
- |               |                                                                                                           |
|---------------|-----------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | In the above reference, refer to Chapter 8, “Troubleshooting the Cisco MGC Node.”                         |
| <b>Step 2</b> | Read the section Media Gateway IP Destination/Link is Out-of-Service and follow the instructions therein. |
-

# Calls Fail at the Cisco MGC

## Description

|                           |                                                                                                                                      |
|---------------------------|--------------------------------------------------------------------------------------------------------------------------------------|
| <b>Summary</b>            | If calls appear to be failing at the Cisco MGC, and the calls are not appearing on the associated media gateway, use this procedure. |
| <b>Target Platform(s)</b> | Cisco MGC (Cisco SC2200 or Cisco PGW 2200)                                                                                           |
| <b>Application</b>        | See <a href="#">Introduction, page 13-1</a>                                                                                          |
| <b>Frequency</b>          | As needed                                                                                                                            |

## Reference

Depends on the solution and related release of the Cisco MGC software. See [References, page 13-2](#).

## Procedure

To resolve a situation where calls are failing at the Cisco MGC:

- 
- |               |                                                                                   |
|---------------|-----------------------------------------------------------------------------------|
| <b>Step 1</b> | In the above reference, refer to Chapter 8, “Troubleshooting the Cisco MGC Node.” |
| <b>Step 2</b> | Read the section Calls Fail at the Cisco MGC and follow the instructions therein. |
-

# Modifying Redundant Link Manager Timers

## Description

|                           |                                                                       |
|---------------------------|-----------------------------------------------------------------------|
| <b>Summary</b>            | Use this procedure to modify the redundant link manager (RLM) timers. |
| <b>Target Platform(s)</b> | Cisco MGC (Cisco SC2200 or Cisco PGW 2200) and Cisco AS5000 series    |
| <b>Application</b>        | See <a href="#">Introduction, page 13-1</a>                           |
| <b>Frequency</b>          | As needed                                                             |

## Reference

Depends on the solution and related release of the Cisco MGC software. See [References, page 13-2](#).

## Procedure

To modify the RLM timers:

- 
- |               |                                                                                               |
|---------------|-----------------------------------------------------------------------------------------------|
| <b>Step 1</b> | In the above reference, refer to Chapter 8, “Troubleshooting the Cisco MGC Node.”             |
| <b>Step 2</b> | Read the section Modifying Redundant Link Manager Timers and follow the instructions therein. |
- 

## Notes

- *Related tasks:* [Rebooting Your System to Modify Properties, page 13-40](#)

# Performing a Call Trace

## Description

|                           |                                                              |
|---------------------------|--------------------------------------------------------------|
| <b>Summary</b>            | Use this procedure to perform a call trace on the Cisco MGC. |
| <b>Target Platform(s)</b> | Cisco MGC (Cisco SC2200 or Cisco PGW 2200)                   |
| <b>Application</b>        | See <a href="#">Introduction, page 13-1</a>                  |
| <b>Frequency</b>          | As needed                                                    |

## Reference

Depends on the solution and related release of the Cisco MGC software. See [References, page 13-2](#).

## Procedure

To perform a call trace:

- 
- |               |                                                                                   |
|---------------|-----------------------------------------------------------------------------------|
| <b>Step 1</b> | In the above reference, refer to Chapter 8, “Troubleshooting the Cisco MGC Node.” |
| <b>Step 2</b> | Read the section Performing a Call Trace and follow the instructions therein.     |
- 

## Notes

- *Related tasks:* [Alternatives to Call Tracing, page 13-31](#)

# Alternatives to Call Tracing

## Description

|                           |                                                                                                                                                                                      |
|---------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Summary</b>            | When you need to perform a call trace to diagnose either a hung call or an abnormally terminated call, and do not want to reduce the performance of your system, use this procedure. |
| <b>Target Platform(s)</b> | Cisco MGC (Cisco SC2200 or Cisco PGW 2200)                                                                                                                                           |
| <b>Application</b>        | See <a href="#">Introduction, page 13-1</a>                                                                                                                                          |
| <b>Frequency</b>          | As needed                                                                                                                                                                            |

## Reference

Depends on the solution and related release of the Cisco MGC software. See [References, page 13-2](#).

## Procedure

To perform an alternative call trace method:

- 
- |               |                                                                                    |
|---------------|------------------------------------------------------------------------------------|
| <b>Step 1</b> | In the above reference, refer to Chapter 8, “Troubleshooting the Cisco MGC Node.”  |
| <b>Step 2</b> | Read the section Alternatives to Call Tracing and follow the instructions therein. |
- 

## Notes

- *Related tasks:* [Performing a Call Trace, page 13-30](#)

# Performing a TCAP Trace

## Description

|                           |                                                              |
|---------------------------|--------------------------------------------------------------|
| <b>Summary</b>            | Use this procedure to perform a TCAP trace on the Cisco MGC. |
| <b>Target Platform(s)</b> | Cisco MGC (Cisco SC2200 or Cisco PGW 2200)                   |
| <b>Application</b>        | See <a href="#">Introduction, page 13-1</a>                  |
| <b>Frequency</b>          | As needed                                                    |

## Reference

Depends on the solution and related release of the Cisco MGC software. See [References, page 13-2](#).

## Procedure

To perform a TCAP trace on the Cisco MGC:

- 
- |               |                                                                                         |
|---------------|-----------------------------------------------------------------------------------------|
| <b>Step 1</b> | In the above reference, refer to Chapter 8, “Troubleshooting the Cisco MGC Node.”       |
| <b>Step 2</b> | Read the section Resolving Performing a TCAP Trace and follow the instructions therein. |
-



# Deleting Unnecessary Files

## Description

|                           |                                                                                                                                                           |
|---------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Summary</b>            | You may need to delete files from your Cisco MGC host(s) to ensure the proper functioning of your system. Use this procedure to delete unnecessary files. |
| <b>Target Platform(s)</b> | Cisco MGC (Cisco SC2200 or Cisco PGW 2200)                                                                                                                |
| <b>Application</b>        | See <a href="#">Introduction, page 13-1</a>                                                                                                               |
| <b>Frequency</b>          | As needed                                                                                                                                                 |

## Reference

Depends on the solution and related release of the Cisco MGC software. See [References, page 13-2](#).

## Procedure

To delete unnecessary files from the disk drives of your Cisco MGC host(s):

- 
- Step 1** In the above reference, refer to Chapter 8, “Troubleshooting the Cisco MGC Node.”
  - Step 2** Read the section Deleting Unnecessary Disk Files to Increase Available Space and follow the instructions therein.
-

# Recovering from a Switchover Failure

## Description

|                           |                                                                                |
|---------------------------|--------------------------------------------------------------------------------|
| <b>Summary</b>            | Use this procedure to recover your Cisco MGC system from a switchover failure. |
| <b>Target Platform(s)</b> | Cisco MGC (Cisco SC2200 or Cisco PGW 2200)                                     |
| <b>Application</b>        | See <a href="#">Introduction, page 13-1</a>                                    |
| <b>Frequency</b>          | As needed                                                                      |

## Reference

Depends on the solution and related release of the Cisco MGC software. See [References, page 13-2](#).

## Procedure

To recover from a switchover failure:

- 
- |               |                                                                                            |
|---------------|--------------------------------------------------------------------------------------------|
| <b>Step 1</b> | In the above reference, refer to Chapter 8, “Troubleshooting the Cisco MGC Node.”          |
| <b>Step 2</b> | Read the section Recovering from a Switchover Failure and follow the instructions therein. |
-

# Recovering from Cisco MGC Host(s) Failure

## Description

|                           |                                                                                                                                                                                                                                             |
|---------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Summary</b>            | There are situations, such as a replacement of a failed disk drive, a 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. |
| <b>Target Platform(s)</b> | Cisco MGC (Cisco SC2200 or Cisco PGW 2200)                                                                                                                                                                                                  |
| <b>Application</b>        | See <a href="#">Introduction, page 13-1</a>                                                                                                                                                                                                 |
| <b>Frequency</b>          | As needed                                                                                                                                                                                                                                   |

## Reference

Depends on the solution and related release of the Cisco MGC software. See [References, page 13-2](#).

## Procedure

To recover from a failed Cisco MGC host or hosts:

- 
- |               |                                                                                                 |
|---------------|-------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | In the above reference, refer to Chapter 8, “Troubleshooting the Cisco MGC Node.”               |
| <b>Step 2</b> | Read the section Recovering from Cisco MGC Host(s) Failure and follow the instructions therein. |
-

# Restoring Stored Configuration Data

## Description

|                           |                                                                                                                                                                                                                                                                                                         |
|---------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Summary</b>            | To resolve problems where the Cisco MGC is not functioning properly as a result of hardware failure, natural disaster, or software corruption, you will need to restore stored configuration data. The steps in this procedure assume that you have been performing regular software backup operations. |
| <b>Target Platform(s)</b> | Cisco MGC (Cisco SC2200 or Cisco PGW 2200)                                                                                                                                                                                                                                                              |
| <b>Application</b>        | See <a href="#">Introduction, page 13-1</a>                                                                                                                                                                                                                                                             |
| <b>Frequency</b>          | As needed                                                                                                                                                                                                                                                                                               |

## Reference

Depends on the solution and related release of the Cisco MGC software. See [References, page 13-2](#).

## Procedure

To restore stored configuration data:



### Caution

To be able to perform this procedure, you must have been backing up the Cisco MGC software on a regular basis. For more information on backing up the Cisco MGC, refer to the Backing Up System Software section in Chapter 3 “Cisco MGC Node Operations” of the appropriate release of the *Cisco Media Gateway Controller Software Operations, Maintenance, and Troubleshooting Guide*.

- 
- Step 1** In the above reference, refer to Chapter 8, “Troubleshooting the Cisco MGC Node.”
- Step 2** Read the section Restoring Stored Configuration Data and follow the steps therein.
- 

## Notes

- *Related tasks:* Backing Up System Software in Chapter 3 “Cisco MGC Node Operations,” of the appropriate release of the *Cisco Media Gateway Controller Software Operations, Maintenance, and Troubleshooting Guide*
- *Related documents:* The appropriate release of the *Cisco Media Gateway Controller Software Operations, Maintenance, and Troubleshooting Guide*

# Verifying Proper Configuration of Replication

## Description

|                           |                                                                                                                                                                       |
|---------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Summary</b>            | If calls are not being preserved when your system performs a switchover, use this procedure to verify that your system is properly configured to replicate call data. |
| <b>Target Platform(s)</b> | Cisco MGC (Cisco SC2200 or Cisco PGW 2200)                                                                                                                            |
| <b>Application</b>        | See <a href="#">Introduction, page 13-1</a>                                                                                                                           |
| <b>Frequency</b>          | As needed                                                                                                                                                             |

## Reference

Depends on the solution and related release of the Cisco MGC software. See [References, page 13-2](#).

## Procedure

To verify that replication has been configured correctly on your system:

- 
- |               |                                                                                                           |
|---------------|-----------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | In the above reference, refer to Chapter 8, “Troubleshooting the Cisco MGC Node.”                         |
| <b>Step 2</b> | Read the section Verification of Proper Configuration of Replication and follow the instructions therein. |
-

# Measurements Are Not Being Generated

## Description

|                           |                                                                             |
|---------------------------|-----------------------------------------------------------------------------|
| <b>Summary</b>            | If your Cisco MGC is not producing system measurements, use this procedure. |
| <b>Target Platform(s)</b> | Cisco MGC (Cisco SC2200 or Cisco PGW 2200)                                  |
| <b>Application</b>        | See <a href="#">Introduction, page 13-1</a>                                 |
| <b>Frequency</b>          | As needed                                                                   |

## Reference

Depends on the solution and related release of the Cisco MGC software. See [References, page 13-2](#).

## Procedure

To configure your system to record system measurements:

- 
- |               |                                                                                        |
|---------------|----------------------------------------------------------------------------------------|
| <b>Step 1</b> | In the above reference, refer to Chapter 8, “Troubleshooting the Cisco MGC Node.”      |
| <b>Step 2</b> | Read the section Measurements Not Being Generated and follow the instructions therein. |
-

# Call Detail Records Are Not Being Generated

## Description

|                           |                                                                                           |
|---------------------------|-------------------------------------------------------------------------------------------|
| <b>Summary</b>            | If call detail records (CDRs) are not being generated by your system, use this procedure. |
| <b>Target Platform(s)</b> | Cisco MGC (Cisco SC2200 or Cisco PGW 2200)                                                |
| <b>Application</b>        | See <a href="#">Introduction, page 13-1</a>                                               |
| <b>Frequency</b>          | As needed.                                                                                |

## Reference

Depends on the solution and related release of the Cisco MGC software. See [References, page 13-2](#).

## Procedure

To configure your system to produce CDRs:

- 
- |               |                                                                                               |
|---------------|-----------------------------------------------------------------------------------------------|
| <b>Step 1</b> | In the above reference, refer to Chapter 8, “Troubleshooting the Cisco MGC Node.”             |
| <b>Step 2</b> | Read the section Call Detail Records Not Being Generated and follow the instructions therein. |
-

# Rebooting Your System to Modify Properties

## Description

|                           |                                                                                                                              |
|---------------------------|------------------------------------------------------------------------------------------------------------------------------|
| <b>Summary</b>            | When you are modifying certain properties on the Cisco MGC, you must reboot your system as part of the modification process. |
| <b>Target Platform(s)</b> | Cisco MGC (Cisco SC2200 or Cisco PGW 2200)                                                                                   |
| <b>Application</b>        | See <a href="#">Introduction, page 13-1</a>                                                                                  |
| <b>Frequency</b>          | As needed                                                                                                                    |

## Reference

Depends on the solution and related release of the Cisco MGC software. See [References, page 13-2](#).

## Procedure

To reboot your Cisco MGC software to modify properties:

- 
- |               |                                                                                                  |
|---------------|--------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | In the above reference, refer to Chapter 8, “Troubleshooting the Cisco MGC Node.”                |
| <b>Step 2</b> | Read the section Rebooting Your System To Modify Properties and follow the instructions therein. |
-



# Resolving a Failed Connection to a Peer

## Description

|                           |                                                                                          |
|---------------------------|------------------------------------------------------------------------------------------|
| <b>Summary</b>            | If you have lost connection to a peer component in your network, perform this procedure. |
| <b>Target Platform(s)</b> | Cisco MGC (Cisco SC2200 or Cisco PGW 2200)                                               |
| <b>Application</b>        | See <a href="#">Introduction, page 13-1</a>                                              |
| <b>Frequency</b>          | As needed                                                                                |

## Reference

Depends on the solution and related release of the Cisco MGC software. See [References, page 13-2](#).

## Procedure

To resolve a failed connection to a peer:

- 
- |               |                                                                                               |
|---------------|-----------------------------------------------------------------------------------------------|
| <b>Step 1</b> | In the above reference, refer to Chapter 8, “Troubleshooting the Cisco MGC Node.”             |
| <b>Step 2</b> | Read the section Resolving a Failed Connection to a Peer and follow the instructions therein. |
-





# Troubleshooting the Cisco Access Registrar

## Introduction

This chapter presents troubleshooting tasks for the Cisco Access Registrar (AR) as they relate to the Cisco ASAP Solution. Cisco AR is discussed in [Chapter 7, “Operating and Maintaining the Cisco Access Registrar.”](#)



### Note

---

This chapter *does not apply* to the Cisco SS7 Interconnect for Voice Gateways Solution.

---

Cisco Access Registrar supports RADIUS proxy. This means that, instead of directly authenticating and authorizing users against a directory, the server selectively proxies the AAA request to another service provider’s RADIUS server or a customer’s RADIUS server, which in turn authenticates and authorizes users against another directory or database.

## Troubleshooting Procedures

- [RADIUS Server Not Defined](#)
- [RADIUS Keys Mismatched](#)
- [Authorization Incorrectly Configured](#)

## Useful IOS Commands

- [Using show Commands](#)
- [Using debug Commands](#)

## References

For detailed information about how to install and configure the Cisco Access Registrar, see the *Cisco Access Registrar 1.7 Installation and Configuration Guide* at the following URL:

[http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cnsar/1\\_7/install/index.htm](http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cnsar/1_7/install/index.htm)

For a description of the Cisco Access Registrar (AR) components and how to use them, including information of how to use the Cisco AR as a proxy server and details about the using the **aregcmd** and **radclient** commands, refer to the *Cisco Access Registrar 1.7 User's Guide* at the following URL:

[http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cnsar/1\\_7/users/index.htm](http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cnsar/1_7/users/index.htm)

For description of the concepts in the Cisco AR, including understanding RADIUS, authentication and authorization, and accounting refer to the *Cisco Access Registrar 1.7 Concepts and Reference Guide* at the following URL:

[http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cnsar/1\\_7/referenc/index.htm](http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cnsar/1_7/referenc/index.htm)

For a description of features and functions that were implemented in Cisco AR Release 1.7, refer to the *Cisco Access Registrar 1.7 Release Notes*:

[http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cnsar/1\\_7/relnote/index.htm](http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cnsar/1_7/relnote/index.htm)

# RADIUS Server Not Defined

## Description

|                           |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|---------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Summary</b>            | <p>This error is seen when users are unable to get connected.</p> <p>The following is an example of system output indicating a “No radius servers defined!” error.</p> <pre>00:34:23: %LINK-3-UPDOWN: Interface Async2/05, changed state to up 00:34:25: RADIUS: ustruct sharecount=1 00:34:25: RADIUS: No radius servers defined! 00:34:25: RADIUS: No valid server found. Trying any viable server 00:34:25: RADIUS: No radius servers defined! 00:34:25: %RADIUS-3-NOSERVERS: No Radius hosts configured. 00:34:25: RADIUS: No response from server 00:34:25: RADIUS: ustruct sharecount=4 00:34:25: RADIUS: No radius servers defined! 00:34:25: RADIUS: No radius servers defined! 00:34:25: RADIUS: No valid server found. Trying any viable server 00:34:25: RADIUS: No radius servers defined!</pre> |
| <b>Target Platform(s)</b> | Sun SPARC systems                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>Application</b>        | See <a href="#">Introduction, page 14-1</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>Frequency</b>          | As needed                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |

## Reference

For all related documentation, see [References, page 14-1](#).

## Procedure

To resolve an archive extraction error, perform the following steps to verify and debug a RADIUS server:

- 
- Step 1** Verify that the RADIUS server(s) defined under the AAA groups are defined globally on the access server, by using the following command:
- ```
radius-server hostname_ip key key
```
- Where:
- *hostname_ip*—The host name or IP address of the system
 - *key*—Associated key
- If the RADIUS server(s) are not globally defined, update the definition on the access server.
- Step 2** Debug RADIUS using the following command:
- ```
debug radius
```

- Step 3** If an error is indicated, correct it. If that resolves the problem, the procedure is complete. Otherwise, proceed to Step 4.
- Step 4** Contact the Cisco TAC for assistance in resolving this problem.
- 

## Notes

- *Related documents:* *Cisco Resource Pool Manager Server Installation Guide*. See [References](#), page 14-1.

# RADIUS Keys Mismatched

## Description

**Summary** Use this procedure when users cannot get connected to the RADIUS server. This occurs when the access server is unable to understand a response it received from the RADIUS server.

The following is an example of system output indicating that the RADIUS keys are mismatched:

```
004180: Nov 6 14:53:00.995 PST: RADIUS: Initial Transmit
Async3/01*Serial1/0:23
 id 85 172.19.50.123:1645, Access-Request, len 129
004181: Nov 6 14:53:00.995 PST: Attribute 4 6 AC13322D
004182: Nov 6 14:53:00.995 PST: Attribute 5 6 00004017
004183: Nov 6 14:53:00.995 PST: Attribute 26 30 0000000902184173
004184: Nov 6 14:53:00.995 PST: Attribute 61 6 00000000
004185: Nov 6 14:53:00.995 PST: Attribute 1 11 6D6F6465
004186: Nov 6 14:53:00.995 PST: Attribute 30 9 35353531
004187: Nov 6 14:53:00.995 PST: Attribute 3 19 01D1CAD7
004188: Nov 6 14:53:00.995 PST: Attribute 6 6 00000002
004189: Nov 6 14:53:00.995 PST: Attribute 7 6 00000001
004190: Nov 6 14:53:00.995 PST: Attribute 44 10 32413030
004191: Nov 6 14:53:00.999 PST: RADIUS: Received from id 85
172.19.50.123:1645,
 Access-Accept, len 64
004192: Nov 6 14:53:00.999 PST: Attribute 6 6 00000002
004193: Nov 6 14:53:00.999 PST: Attribute 7 6 00000001
004194: Nov 6 14:53:00.999 PST: Attribute 26 32 00000009011A6970
004195: Nov 6 14:53:00.999 PST: RADIUS: Response (85) failed decrypt
004196: Nov 6 14:53:00.999 PST: RADIUS: Reply for 85 fails decrypt
004197: Nov 6 14:53:00.999 PST: AAA/AUTHEN (3934272825): status = ERROR
```

**Target Platform(s)** Sun SPARC systems

**Application** See [Introduction, page 14-1](#)

**Frequency** As needed

## Reference

For all related documentation, see [References, page 14-1](#).

## Procedure

To resolve a mismatch in the RADIUS keys, perform the following steps:

- 
- Step 1** Ensure that the keys for the RADIUS server and the access server match, using the following command:
- ```
debug radius
```
- If the response to the command indicates that the keys match, proceed to Step 3. Otherwise, proceed to Step 2.
- Step 2** Modify the key on the access server to match the key on the RADIUS server.
- If that resolves the problem, the procedure is complete. Otherwise, proceed to Step 3.
- Step 3** Contact the Cisco TAC for assistance in resolving this problem.
-

Notes

- *Related documents:* *Cisco Resource Pool Manager Server Installation Guide*. See [References](#), page 14-1.

Authorization Incorrectly Configured

Description

Summary

Use this procedure when per-user attributes (for example, access lists, filters, and timeouts) are not being applied. The RADIUS server is returning attributes but you do not see them being applied.

The following is an example of system output indicating that the session timeout is not being applied:

```
01:42:33: RADIUS: Received from id 49 171.71.3.40:1645, Access-Accept,
len 38
01:42:33:         Attribute 7 6 00000001
01:42:33:         Attribute 6 6 00000002
01:42:33:         Attribute 27 6 0000003C
01:42:33: AAA/AUTHEN (1378082205): status = PASS
01:42:33: As2/17 AAA/AUTHOR/LCP: Authorize LCP
01:42:33: As2/17 AAA/AUTHOR/LCP (122768983): Port='Async2/17' list=''
service=NET
01:42:33: AAA/AUTHOR/LCP: As2/17 (122768983) user='1_1_2'
01:42:33: As2/17 AAA/AUTHOR/LCP (122768983): send AV service=ppp
01:42:33: As2/17 AAA/AUTHOR/LCP (122768983): send AV protocol=lcp
01:42:33: As2/17 AAA/AUTHOR/LCP (122768983): found list "default"
01:42:33: As2/17 AAA/AUTHOR/LCP (122768983): Method=IF_AUTHEN
01:42:33: As2/17 AAA/AUTHOR (122768983): Post authorization status =
PASS_ADD
```

```
5400#sh caller timeouts
```

Session	Idle	Disconnect	Timeout	Timeout	User in
Line	User		Timeout	Timeout	User in
vty 0	cisco		-	-	-
tty 344	1_1_2		-	-	-
As2/20	1_1_2	00:00:00	3w3d	3w3d	

The example below shows a system response that indicates the session timeout is applied following an authorization setup from the AAA server.

```
02:04:09: RADIUS: Received from id 61 171.71.3.40:1645, Access-Accept,
len 38
02:04:09:         Attribute 7 6 00000001
02:04:09:         Attribute 6 6 00000002
02:04:09:         Attribute 27 6 0000003C
02:04:09: AAA/AUTHEN (3360630259): status = PASS
02:04:09: As2/21 AAA/AUTHOR/LCP: Authorize LCP
02:04:09: As2/21 AAA/AUTHOR/LCP (2560550781): Port='Async2/21' list=''
service=NET
02:04:09: AAA/AUTHOR/LCP: As2/21 (2560550781) user='1_1_2'
02:04:09: As2/21 AAA/AUTHOR/LCP (2560550781): send AV service=ppp
02:04:09: As2/21 AAA/AUTHOR/LCP (2560550781): send AV protocol=lcp
02:04:09: As2/21 AAA/AUTHOR/LCP (2560550781): found list "default"
02:04:09: As2/21 AAA/AUTHOR/LCP (2560550781): Method=MyProxy (radius)
02:04:09: As2/21 AAA/AUTHOR (2560550781): Post authorization status =
PASS_REPL
02:04:09: As2/21 AAA/AUTHOR/LCP: Processing AV service=ppp
02:04:09: As2/21 AAA/AUTHOR/LCP: Processing AV timeout=60
```

```

5400#sh caller timeouts
                                     Session  Idle
Disconnect
Line      User      Timeout  Timeout  User in
vty 0    cisco    -        -        -
tty 344  1_1_2    -        -        -
As2/20   1_1_2    00:01:00 3w3d    00:00:46

ll.java:558)
**ERROR failed to install

```

Target Platform(s)	Sun SPARC systems
Application	See Introduction, page 14-1
Frequency	As needed

Reference

For all related documentation, see [References, page 14-1](#).

Procedure

To correct an AAA authorization problem, perform the following steps:

-
- Step 1** Enter the following command to debug the AAA authorization settings:
- ```
debug aaa authorization
```
- Ensure that the AAA authorization method list points to the AAA server group that contains the per-user attribute information. If the list points to the correct AAA server group, proceed to Step 3. Otherwise, proceed to Step 2.
- Step 2** Modify the AAA authorization method list to point to the AAA server group that contains the per-user attribute information.
- If that resolves the problem, the procedure is complete. Otherwise, proceed to Step 3.
- Step 3** Verify the user profile settings on the AAA server.
- If the user profile settings are correct, proceed to Step 5. Otherwise, proceed to Step 4.
- Step 4** Correct the user profile settings on the AAA server.
- If that resolves the problem, the procedure is complete. Otherwise, proceed to Step 5.
- Step 5** Contact the Cisco TAC for assistance in resolving this problem.
- 

## Notes

- *Special issues:* This problem may also be due to the user profile being incorrectly configured on the AAA server.

# Using show Commands

## Description

|                           |                                                             |
|---------------------------|-------------------------------------------------------------|
| <b>Summary</b>            | Use <b>show</b> commands to troubleshoot Cisco AR problems. |
| <b>Target Platform(s)</b> | Sun SPARC systems                                           |
| <b>Application</b>        | See <a href="#">Introduction, page 14-1</a>                 |
| <b>Frequency</b>          | As needed                                                   |

## Reference

For all related documentation, see [References, page 14-1](#).

## Command

Use the following **show** command:

```
show radius statistics
```

The system returns a response similar to the following:

```
5400-3-pop#sh radius statistics
 Auth. Acct. Both
Maximum inQ length: NA NA 1
Maximum waitQ length: NA NA 2
Maximum doneQ length: NA NA 1
Total responses seen: 6 24 30
Packets with responses: 6 24 30
Packets without responses: 0 10 10
Average response delay(ms): 6 240 193
Maximum response delay(ms): 16 3764 3764
Number of Radius timeouts: 0 41 41
Duplicate ID detects: 0 0 0
```

## Notes

- *Related documents:* *Cisco Resource Pool Manager Server Installation Guide*. See [References, page 14-1](#).

# Using debug Commands

## Description

|                           |                                                              |
|---------------------------|--------------------------------------------------------------|
| <b>Summary</b>            | Use <b>debug</b> commands to troubleshoot Cisco AR problems. |
| <b>Target Platform(s)</b> | Sun SPARC systems                                            |
| <b>Application</b>        | See <a href="#">Introduction, page 14-1</a>                  |
| <b>Frequency</b>          | As needed                                                    |

## Reference

For all related documentation, see [References, page 14-1](#).

## Commands

Use the following **debug** commands:

- **debug aaa authentication**
- **debug aaa authorization**
- **debug aaa accounting**
- **debug radius**

**Tip**

---

Be sure to use conditional debugs (where possible) to minimize the amount of output. The **conditional debug** facility allows a debug command to be triggered by a specific event, such as a user ID or phone number, and turns on debug for the affected port only, enabling problems to be identified and resolved rapidly.

---

**Caution**

---

Do not enable console logging. Instead, log to a buffer or to a syslog server.

---

## Notes

- *Related documents:* *Cisco Resource Pool Manager Server Installation Guide*. See [References, page 14-1](#).



# Troubleshooting Using the Cisco Universal Gateway Manager

## Introduction

This chapter presents troubleshooting tasks related to the Cisco ASAP Solution that are provided from the Cisco Universal Gateway Manager (Cisco UGM), Version 2.0. Cisco UGM is discussed in [Chapter 4, “Managing Network Objects: Using Cisco UGM.”](#) This chapter does not discuss troubleshooting related to installations and upgrades.



**Note**

---

This chapter *does not apply* to the Cisco SS7 Interconnect for Voice Gateways Solution.

---



**Note**

---

The features of Cisco UGM as they relate to the Cisco ASAP Solution are introduced in the *Cisco ASAP Solution Overview and Planning Guide* at the following URL:  
<http://www.cisco.com/univercd/cc/td/doc/product/access/solution/asap/index.htm>

---

The major tasks in this chapter are listed below.

- [Setting Controller Logging Levels](#)
- [Managing Log Files](#)
- [Setting Controller Logging Levels](#)
- [Troubleshooting Configuration and Image Management](#)
- [Troubleshooting Fault Management](#)
- [Troubleshooting Performance Management](#)
- [Troubleshooting the Configure Administrative State Function](#)
- [Troubleshooting IOS Operations](#)



**Note**

---

This chapter does not discuss troubleshooting related to installations and upgrades, although that topic is covered in the referenced document.

---

## References

For the following procedures, refer to Chapter 4, “Troubleshooting Cisco UGM,” of the *Cisco Universal Gateway Manager 2.0 Installation, Upgrade, and Troubleshooting Guide* at the following URL:

<http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/ugm/ugm2/install/index.htm>

# Setting Controller Logging Levels

## Description

|                           |                                                                                                                                               |
|---------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Summary</b>            | Setting the appropriate levels of controller logging is a useful aid in troubleshooting. Use this procedure to set controller logging levels. |
| <b>Target Platform(s)</b> | Cisco AS5350, Cisco AS5400, Cisco AS5800, Cisco AS5850                                                                                        |
| <b>Application</b>        | See <a href="#">Introduction, page 15-1</a>                                                                                                   |
| <b>Frequency</b>          | As needed                                                                                                                                     |

## Reference

Chapter 4, “Troubleshooting Cisco UGM,” of the *Cisco Universal Gateway Manager 2.0 Installation, Upgrade, and Troubleshooting Guide*

## Procedure

To set controller logging levels:

- 
- |               |                                                                                |
|---------------|--------------------------------------------------------------------------------|
| <b>Step 1</b> | In the above-referenced chapter, read Overview of Controller Logging Levels.   |
| <b>Step 2</b> | Read Setting the Controller Logging Level and follow the instructions therein. |
-

# Managing Log Files

## Description

|                           |                                                                                                                                                                                                                                                                 |
|---------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Summary</b>            | It is important to know where log files reside. You can also change the size of various log files and load them. In addition, <i>.ini</i> files contain parameters relevant to the discovery and deployment of devices. Use this procedure to manage log files. |
| <b>Target Platform(s)</b> | Cisco AS5350, Cisco AS5400, Cisco AS5800, Cisco AS5850                                                                                                                                                                                                          |
| <b>Application</b>        | See <a href="#">Introduction, page 15-1</a>                                                                                                                                                                                                                     |
| <b>Frequency</b>          | As needed                                                                                                                                                                                                                                                       |

## Reference

Chapter 4, “Troubleshooting Cisco UGM,” of the *Cisco Universal Gateway Manager 2.0 Installation, Upgrade, and Troubleshooting Guide*

## Procedure

To manage log files:

- 
- Step 1** In the above-referenced chapter, read About Viewing Log Files.
- Step 2** As appropriate, read the instructions in one or more of the following sections and follow the steps therein:
- Changing the Size of ASMainCtrl, IOSConfigCtrl, IASFaultStandAlone, or ASPerformInv Log files
  - Loading historyCriteria Files
  - About .ini Files
-



# Troubleshooting Discovery and Deployment

## Description

|                           |                                                                                              |
|---------------------------|----------------------------------------------------------------------------------------------|
| <b>Summary</b>            | Recovery procedures are provide for a variety of errors related to discovery and deployment. |
| <b>Target Platform(s)</b> | Cisco AS5350, Cisco AS5400, Cisco AS5800, Cisco AS5850                                       |
| <b>Application</b>        | See <a href="#">Introduction, page 15-1</a>                                                  |
| <b>Frequency</b>          | As needed                                                                                    |

## Reference

Chapter 4, “Troubleshooting Cisco UGM,” of the *Cisco Universal Gateway Manager 2.0 Installation, Upgrade, and Troubleshooting Guide*

## Procedure

To troubleshoot discovery and deployment errors:

- 
- Step 1** In the above-referenced chapter, read Troubleshooting Discovery and Deployment.
- Step 2** As appropriate, read the instructions in one or more of the following sections and follow the steps or advice therein:
- Deployment Failed
  - Subchassis deployment failure due to UGM/CEMF internal error
  - Subchassis discovery failed due to UGM/CEMF internal errors
  - Subchassis deployment failed due to internal error
  - Subchassis discovery failed due to loss of communication with device
  - Locating Undiscovered Devices
  - Manual Deployment Failure
  - Consecutive Deployment and Discovery Failures
  - Manual Deployment Failure due to sysOID Mismatch
  - Loss of Communication with a Device
  - Device Rediscovery is Initiated Frequently
  - Redundancy Handover Problem
-

# Troubleshooting Configuration and Image Management

## Description

|                           |                                                                                                         |
|---------------------------|---------------------------------------------------------------------------------------------------------|
| <b>Summary</b>            | Recovery procedures are provided for a variety of errors related to configuration and image management. |
| <b>Target Platform(s)</b> | Cisco AS5350, Cisco AS5400, Cisco AS5800, Cisco AS5850                                                  |
| <b>Application</b>        | See <a href="#">Introduction, page 15-1</a>                                                             |
| <b>Frequency</b>          | As needed                                                                                               |

## Reference

Chapter 4, “Troubleshooting Cisco UGM,” of the [Cisco Universal Gateway Manager 2.0 Installation, Upgrade, and Troubleshooting Guide](#)

## Procedure

To troubleshoot configuration and image management errors:

- 
- |               |                                                                                                                             |
|---------------|-----------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | In the above-referenced chapter, read Troubleshooting Configuration and Image Management.                                   |
| <b>Step 2</b> | Read the descriptions of the error messages that match the condition to be remedied and follow the steps or advice therein. |
-

# Troubleshooting Fault Management

## Description

|                           |                                                                                       |
|---------------------------|---------------------------------------------------------------------------------------|
| <b>Summary</b>            | Recovery procedures are provided for a variety of errors related to fault management. |
| <b>Target Platform(s)</b> | Cisco AS5350, Cisco AS5400, Cisco AS5800, Cisco AS5850                                |
| <b>Application</b>        | See <a href="#">Introduction, page 15-1</a>                                           |
| <b>Frequency</b>          | As needed                                                                             |

## Reference

Chapter 4, “Troubleshooting Cisco UGM,” of the *Cisco Universal Gateway Manager 2.0 Installation, Upgrade, and Troubleshooting Guide*

## Procedure

To troubleshoot fault management errors:

- 
- Step 1** In the above-referenced chapter, read Troubleshooting Fault Management.
- Step 2** As appropriate, read the instructions in one or more of the following sections and follow the steps or advice therein:
- Troubleshooting Missing Events from a Device
  - Troubleshooting Trap Forwarding
  - Troubleshooting Missing Events from the Event Browser
  - Cisco UGM Does Not Raise Alarms upon Receiving Traps
-

# Troubleshooting Performance Management

## Description

|                           |                                                                                             |
|---------------------------|---------------------------------------------------------------------------------------------|
| <b>Summary</b>            | Recovery procedures are provided for a variety of errors related to performance management. |
| <b>Target Platform(s)</b> | Cisco AS5350, Cisco AS5400, Cisco AS5800, Cisco AS5850                                      |
| <b>Application</b>        | See <a href="#">Introduction, page 15-1</a>                                                 |
| <b>Frequency</b>          | As needed                                                                                   |

## Reference

Chapter 4, “Troubleshooting Cisco UGM,” of the [Cisco Universal Gateway Manager 2.0 Installation, Upgrade, and Troubleshooting Guide](#)

## Procedure

To troubleshoot performance management errors:

- 
- Step 1** In the above-referenced chapter, read Troubleshooting Performance Management.
- Step 2** As appropriate, read the instructions in one or more of the following sections and follow the steps or advice therein:
- Missed Poll
  - Changing Polling Period Intervals
  - Stopping Performance Polling on Devices
  - Performance Polling Configuration Dialog shows Polling Intervals for MIBs and MIB Attributes in Cisco UGM 1.0
  - Error: You must be logged in as root to run the scripts
  - Performance Manager contains no Data for Attributes
  - Error: Object has no attributes that are being monitored
  - No Data is Exported to File
  - File Aging Actions are not Completed
  - Performance Manager shows no Polling Activity
  - Changing the Polling Interval does not Affect Performance Manager Operation
  - Polling raises an Alarm and places the Device in Status 4
-

# Troubleshooting the Configure Administrative State Function

## Description

|                           |                                                                                                                  |
|---------------------------|------------------------------------------------------------------------------------------------------------------|
| <b>Summary</b>            | Recovery procedures are provided for a variety of errors related to the Configure Administrative State function. |
| <b>Target Platform(s)</b> | Cisco AS5350, Cisco AS5400, Cisco AS5800, Cisco AS5850                                                           |
| <b>Application</b>        | See <a href="#">Introduction, page 15-1</a>                                                                      |
| <b>Frequency</b>          | As needed                                                                                                        |

## Reference

Chapter 4, “Troubleshooting Cisco UGM,” of the *Cisco Universal Gateway Manager 2.0 Installation, Upgrade, and Troubleshooting Guide*

## Procedure

To troubleshoot errors related to the Configure Administrative State function:

- 
- Step 1** In the above-referenced chapter, read Troubleshooting the Configure Administrative State function.
- Step 2** As appropriate, read the instructions in one or more of the following sections and follow the steps or advice therein:
- Correcting Ping Failure
  - Unexpected Dialog Box Updates
  - Graceful Shutdown Interrupted and Accept Traffic Interrupted
  - False Completion
  - Graceful Shutdown Alarm
  - Accepting Traffic Failure
-

# Troubleshooting IOS Operations

## Description

|                           |                                                                                     |
|---------------------------|-------------------------------------------------------------------------------------|
| <b>Summary</b>            | Recovery procedures are provided for a variety of errors related to IOS operations. |
| <b>Target Platform(s)</b> | Cisco AS5350, Cisco AS5400, Cisco AS5800, Cisco AS5850                              |
| <b>Application</b>        | See <a href="#">Introduction, page 15-1</a>                                         |
| <b>Frequency</b>          | As needed                                                                           |

## Reference

Chapter 4, “Troubleshooting Cisco UGM,” of the *Cisco Universal Gateway Manager 2.0 Installation, Upgrade, and Troubleshooting Guide*

## Procedure

To troubleshoot errors related to IOS operations:

- 
- Step 1** In the above-referenced chapter, read Troubleshooting IOS Operations.
- Step 2** As appropriate, read the instructions in one or more of the following sections and follow the steps or advice therein:
- ERROR: logging in. Invalid password
  - ERROR: No response from device
  - ERROR: Unable to connect. Port may be in use or inaccessible
-



# Troubleshooting the Cisco RPMS

## Introduction

This chapter presents operations and maintenance tasks related to the Cisco ASAP Solution that are provided from Cisco RPMS Release 1.1 *only*. Cisco RPMS Release 2.0 is discussed in [Chapter 3, “Managing Resources and Dial Services: Using Cisco RPMS.”](#)



**Note**

This chapter *does not apply* to the PSTN gateway solutions and the Cisco PSTN Gateway Solution only supports RPMS using dial calls.



**Note**

Procedures for troubleshooting Cisco RPMS Release 2.0 will be provided as they become available.

The main focus of this troubleshooting chapter is on the GUI form of the application. However, where CLI commands are applicable, the reader is referred to related commands. CLI commands can be run only on the host machine.



**Note**

The features of Cisco RPMS as they relate to the Cisco ASAP Solution are introduced in the *Cisco ASAP Solution Overview and Planning Guide*.

With this application you can configure call discrimination, configure resource management, configure dial services, view server reports, and administer the server. The tasks in this chapter are listed below.

## System Installation and Startup

- [Archive Extraction Error](#)
- [Database Initialization Failure](#)
- [Database Connectivity Failure](#)
- [Web Server Fails to Start](#)
- [Unable to Start/Stop Oracle](#)
- [Unable to Start/Stop TNS Listener](#)

## GUI Access

- [Images on the Cisco RPMS GUI Are Not Displayed Correctly](#)
- [Unable to Add/Change/Delete Administrators in the GUI](#)

## Operational Problems

- [RPMS Server Process Is Not Running](#)
- [RPMS Database Server Process Is Not Running](#)
- [RPMS Watchdog Process Is Not Running](#)
- [Incorrect Access Server and Cisco RPMS Keys](#)
- [Cisco RPMS Cannot Identify Access Server](#)
- [TACACS+ Single Connection Is Configured](#)
- [Port Counts Are Out of Synchronization](#)
- [Oracle Configuration Updates Are Not Reflected on Snapshot Site Cisco RPMS Server\(s\)](#)
- [Enabling a Cisco RPMS Debugging Session](#)
- [Disabling a Cisco RPMS Debugging Session](#)

## Related IOS Commands

- [Using show Commands](#)
- [Using debug Commands](#)

## References

For the following procedures, refer to Cisco Resource Pool Manager Server 1.1 at the following URL:

[http://www.cisco.com/univercd/cc/td/doc/product/access/acs\\_soft/rpms/rpms\\_1-1/index.htm](http://www.cisco.com/univercd/cc/td/doc/product/access/acs_soft/rpms/rpms_1-1/index.htm)

The following documents there are referenced:

- *Cisco Resource Pool Manager Server 1-1 Installation Guide*
- *Cisco Resource Pool Manager Server 1-1 Configuration Guide*
- *Cisco Resource Pool Manager Server 1-1 Solutions Guide*

Make sure you are familiar with the above documents.



# Archive Extraction Error

## Description

**Summary** An archive extraction error happens because the program `./installcrpms` is not able to run because it is unable to open a window to show the install instructions and accept install parameters from the user. This is because the X Server running in the Solaris host is not accepting the request (possibly for security reasons) from the `./installcrpms` to open an X Window.

**Note** The user may see a very similar error while running the `./uninstallcrpms` command. This is because the uninstall program also needs to open up a window. The solution is the same.

**Note** This problem may also be encountered during un-installation

The following is an example of system output indicating an archive extraction error:

```
0) I want to specify a path to an interpreter.
1) Use /router/bin/java
2) Use /router/bin/jre
3) Use /usr/bin/java
4) Use /usr/bin/jre
5) Terminate this installation.
Select a choice [0-5]: 2
Extracting installation class
InstallShield Java (TM) Edition
Extracting installation code.....done
Unable to extract this archive.
java.lang.NoClassDefFoundError
java.lang.RuntimeException
 at installcrpms.bail(install.java:526)
 at installcrpms.execute(install.java:346)
 at installcrpms.<init>(install.java:140)
 at installcrpms.main(install.java:558)
**ERROR failed to install
```

**Target Platform(s)** Cisco AS5000 series

**Application** See [Introduction, page 16-1](#)

**Frequency** As needed

## Reference

*Cisco Resource Pool Manager Server 1-1 Installation Guide*

For all related documents, see [References, page 16-2](#).

## Procedure

To resolve an archive extraction error, perform the following steps:

---

**Step 1** Ensure that the DISPLAY variable is set properly, by using the following command:

```
setenv DISPLAY <IP address> | <hostname>:0.0
```

Where

- *IP address*—is the IP address of your system
- *hostname*—is the host name of your system

**Step 2** Verify that X Windows access control is enabled, by using the following command:

```
/usr/openwin/bin/xhost +
```

**Step 3** Reattempt an installation of the Cisco RPMS software. Refer to the *Cisco Resource Pool Manager Server 1-1 Installation Guide* for details.

If the database initialization error occurs again, proceed to Step 4.

**Step 4** Contact the Cisco TAC for assistance.

---

# Database Initialization Failure

## Description

**Summary** A database can fail to be initialized when you downgrade Cisco RPMS from a higher release.



**Warning** **Downgrading from Cisco RPMS 1.1 is NOT recommended.**

The following is an example of system output indicating a database initialization error:

```
"Failed to initialize the database, please review the log file
/tmp/rpmsinstall.log and follow the recommendations at the bottom of the
log file to correct the problem. After the problem has been corrected,
uninstall by executing a file called /export/home/crpms/uninstallcrpms,
and then reinstall the product".
```

**Target Platform(s)** Cisco AS5000 series

**Application** See [Introduction, page 16-1](#)

**Frequency** As needed

## Reference

*[Cisco Resource Pool Manager Server 1-1 Installation Guide](#)*

For all related documents, see [References, page 16-2](#).

## Procedure

To resolve a database initialization failure, perform the following steps:

**Step 1** Enter the following command to see the installation log:

```
tail /tmp/rpmsinstall.log
```

The system returns a response similar to the following:

```
Loading properties from /export/home/crpms/sbin/./config/dbserver.conf
Finished loading properties.
Data Source = ORACLE
Driver Type = JDBC-Weblogic-Oracle URL = jdbc:weblogic:oracle:rpms_db username = rpms
password = *****
```

```
Connected to jdbc:weblogic:oracle:rpms_db
Driver Weblogic, Inc. Java-OCI JDBC Driver (weblogicoci26)
```

```
Version 2.5.4

Current schema version: 7
Current RPMS schema version: 10
Current RPMS schema (10) is not up to date for upgrade
Upgrading schema failed.
Upgrading schema failed.

Failed.
```

**Step 2** If you are not downgrading Cisco RPMS from a higher release, proceed to Step 4. Otherwise, manually remove the Cisco RPMS database tables by using the following commands:

```
rlogin localhost -l oracle
<RPMS_home_dir>/sbin/csdbtool drop
<RPMS_home_dir>/sbin/ csdbtool drop_rpms
```

**Step 3** Reattempt an installation of the Cisco RPMS software. Refer to the *Cisco Resource Pool Manager Server Installation Guide* for details.

If the database initialization error occurs again, proceed to Step 4.

**Step 4** Contact the Cisco TAC for assistance.

---

# Database Connectivity Failure

## Description

**Summary** A database connectivity failure occurs when Cisco RPMS is unable to connect with the database.

**Note** The user may see a very similar error while running the `./uninstallcrpms` command. This is because the uninstall program also needs to open up a window. The solution is the same.

**Note** This problem may also be encountered during uninstallation.

The following is an example of system output indicating an database connectivity error:

```

Loading properties from /opt/app/rpms/sbin/./config/dbserver.conf
Finished loading properties.
Data Source = ORACLE
Driver Type = JDBC-Weblogic-Oracle URL = jdbc:weblogic:oracle:globedb
 username = oracle password = *****
DBFactory Error: driver was unable to connect to the data source, driver
msg:[ORA-01017: invalid username/password; logon denied
-(oracle/*****@globedb)]

```

**Target Platform(s)** Cisco AS5000 series

**Application** See [Introduction, page 16-1](#)

**Frequency** As needed

## Reference

*Cisco Resource Pool Manager Server 1-1 Installation Guide*

For all related documents, see [References, page 16-2](#).

## Procedure

To resolve a database connectivity failure, perform the following steps:

**Step 1** Verify that the database is not connecting to Cisco RPMS by entering the following commands:

```

rlogin localhost -l oracle
cd <Oracle_home_dir>/bin
./sqlplus rpmsuser/<password>@<TNS_name>
./tnsping <TNS_name>

```

If the response to these commands indicates that Cisco RPMS is not connecting to the database, proceed to Step 2. Otherwise, proceed to Step 9.

**Step 2** Verify the status of the TNS Listener by entering the following command:

```
./lsnrctl status
```

**Step 3** If a failure is indicated, start TNS Listener manually by using the following command:

```
<Oracle_home_dir>/bin/lsnrctl start
```

If TNS Listener restarts, proceed to Step 4. Otherwise, proceed to Step 5.

**Step 4** Repeat Step 1 to verify database connectivity.

**Step 5** If TNS listener does not restart, restart Oracle:

```
rlogin localhost -l oracle
<Oracle_home_dir>/bin/svrmgrl
connect internal;
startup
exit
```

**Step 6** Restart TNS Listener.

**Step 7** Repeat Step 1 to verify database connectivity.

**Step 8** Reattempt an installation of the Cisco RPMS software. Refer to the *Cisco Resource Pool Manager Server Installation Guide* for details.

If the database initialization error occurs again, proceed to Step 9.

**Step 9** Contact the Cisco TAC for assistance.

---

## Notes

- *Related tasks:* [Archive Extraction Error, page 16-3](#)

# Web Server Fails to Start

## Description

|                           |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|---------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Summary</b>            | <p>This problem occurs when the Web server fails to start during Cisco RPMS startup. The following is an example of system output indicating that the Web server failed to start:</p> <pre>host# sbin/crpms start Starting Cisco RPM Server on Wed May 30 17:33:45 PDT 2001 Note: using VM "/export/home/crpms/java/bin/jre" Java VM version 1.1.7 Starting RPMS Database Server... DBServer Started Starting RPMS... RPMS Started Starting administrative servlets... Admin Servlets Started Starting Fast Track Admin Web server could not bind to port 64000 (Address already in use) Fast Track Admin Web server Failed to start</pre> |
| <b>Target Platform(s)</b> | Cisco AS5000 series                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Application</b>        | See <a href="#">Introduction, page 16-1</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>Frequency</b>          | As needed                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |

## Reference

*Cisco Resource Pool Manager Server 1-1 Installation Guide*

For all related documents, see [References, page 16-2](#).

## Procedure

To return the Web server to service, perform the following steps:

- 
- |               |                                                                                                                       |
|---------------|-----------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | Stop the Web server by using the following command:<br><pre>&lt;RPMS_home_dir&gt;/sbin/crpms webserver stop</pre>     |
| <b>Step 2</b> | Restart the Web server by using the following command:<br><pre>&lt;RPMS_home_dir&gt;/sbin/crpms webserver start</pre> |
| <b>Step 3</b> | If the Web server restarts, the procedure is complete. Otherwise, contact the Cisco TAC for assistance.               |
-

# Unable to Start/Stop Oracle

## Description

|                           |                                                                                                                                                                                                                                                                                                                                                                                                           |
|---------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Summary</b>            | This problem occurs when the system is unable to start or stop the Oracle database. The following is an example of system output indicating a database connectivity error:<br><br><pre>host# bin/svrmgrl stop Oracle Server Manager Release 3.0.5.0.0 - Production Message 4505 not found; No message file for product=SVRMGR, facility=MGR Error while trying to retrieve text for error ORA-12571</pre> |
| <b>Target Platform(s)</b> | Cisco AS5000 series                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Application</b>        | See <a href="#">Introduction, page 16-1</a>                                                                                                                                                                                                                                                                                                                                                               |
| <b>Frequency</b>          | As needed                                                                                                                                                                                                                                                                                                                                                                                                 |

## Reference

*Cisco Resource Pool Manager Server 1-1 Installation Guide*

For all related documents, see [References, page 16-2](#).

## Procedure

To start or stop the Oracle database, perform the following steps:

---

**Step 1** Ensure that you are logged in as an Oracle user by entering the following commands:

```
id
uid=1002(oracle) gid=101(dba)
```

If you are logged in, proceed to Step 3. Otherwise, proceed to Step 2.

**Step 2** Log in as an Oracle user by using the following command:

```
rlogin localhost -l oracle
```

**Step 3** Ensure that the environmental variables are inherited by entering the following command:

```
env
```

The system should return a response similar to the following:

```
HOME=/export/home/oracle
PATH=/bin:/usr/bin:/usr/sbin:/usr/ucb:/usr/openwin/bin:/usr/dt/bin:/etc/./opt/app/oracle/
product/8.0.5/bin:/opt/app/oracle/product/8.0.5/sbin:/opt/app/rpms/bin
LOGNAME=oracle
HZ=100
```



```
TERM=vt100
TZ=US/Pacific
SHELL=/bin/csh
MAIL=/var/mail/oracle
PWD=/export/home/oracle
USER=oracle
ORACLE_BASE=/opt/app/oracle
ORACLE_HOME=/opt/app/oracle/product/8.0.5
ORACLE_DOC=/opt/app/oracle/doc
ORACLE_SID=epicurus
ORACLE_TERM=xsun5
ORACLE_PATH=/opt/app/oracle/product/8.0.5/bin:/opt/bin:/bin:/usr/bin:/usr/ccs/bin
ORACLE_OWNER=oracle
LD_LIBRARY_PATH=/opt/app/oracle/product/8.0.5/lib:/usr/openwin/lib:/usr/dt/lib:/usr/lib:/usr/local/lib
TMPDIR=/var/tmp
DISPLAY=epicurus:0.0
```

**Step 4** If the response is not similar, ensure that the Oracle variables are defined in the Oracle user file *.cshrc* (according to the installation guide) and reinstate variables by using the following command:

```
source .cshrc
```

**Step 5** If the Web server restarts, the procedure is complete. Otherwise, contact the Cisco TAC for assistance.

---

# Unable to Start/Stop TNS Listener

## Description

|                           |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|---------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Summary</b>            | Used when an error message is received when trying to start or stop TNS Listener.<br>The following is an example of system output indicating a problem with the TNS Listener:<br><br><pre>host# bin/lsnrctl stop LSNRCTL for Solaris: Version 8.0.5.0.0 - Production on 21-JUL-01 15:40:41 (c) Copyright 1997 Oracle Corporation. All rights reserved. Message 1053 not found; No message file for product=NETWORK, facility=TNSMessage 1052 not found; No message file for product=NETWORK, facility=TNS</pre> |
| <b>Target Platform(s)</b> | Cisco AS5000 series                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>Application</b>        | See <a href="#">Introduction, page 16-1</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>Frequency</b>          | As needed                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |

## Reference

*Cisco Resource Pool Manager Server 1-1 Installation Guide*

For all related documents, see [References, page 16-2](#).

## Procedure

To start or stop the TNS Listener, perform the following steps:

- 
- Step 1** Ensure that you are logged in as an Oracle user by entering the following command:
- ```
id
uid=1002(oracle) gid=101(dba)
```
- Step 2** If the response indicates that you are not logged in, log in as an Oracle user by entering the following command:
- ```
rlogin localhost -l oracle
```
- Step 3** Ensure that the environmental variables are inherited by entering the following command:
- ```
env
```

The system should return a response similar to the following:

```
HOME=/export/home/oracle
PATH=/bin:/usr/bin:/usr/sbin:/usr/ucb:/usr/openwin/bin:/usr/dt/bin:/etc/./opt/app/oracle/
product/8.0.5/bin:/opt/app/oracle/product/8.0.5/sbin:/opt/app/rpms/bin
```

```
LOGNAME=oracle
HZ=100
TERM=vt100
TZ=US/Pacific
SHELL=/bin/csh
MAIL=/var/mail/oracle
PWD=/export/home/oracle
USER=oracle
ORACLE_BASE=/opt/app/oracle
ORACLE_HOME=/opt/app/oracle/product/8.0.5
ORACLE_DOC=/opt/app/oracle/doc
ORACLE_SID=epicurus
ORACLE_TERM=xsun5
ORACLE_PATH=/opt/app/oracle/product/8.0.5/bin:/opt/bin:/bin:/usr/bin:/usr/ccs/bin
ORACLE_OWNER=oracle
LD_LIBRARY_PATH=/opt/app/oracle/product/8.0.5/lib:/usr/openwin/lib:/usr/dt/lib:/usr/lib:/usr/local/lib
TMPDIR=/var/tmp
DISPLAY=epicurus:0.0
```

Step 4 If the response is not similar, ensure that the Oracle variables are defined in the Oracle user file `.cshrc` (according to the installation guide) and apply variables by using the following command:

```
source .cshrc
```

Step 5 If the Web server restarts, the procedure is complete. Otherwise, contact the Cisco TAC for assistance.

Images on the Cisco RPMS GUI Are Not Displayed Correctly

Description

Summary	Use this technique when images on the GUI for the RPMS are not displaying correctly.
Target Platform(s)	Cisco AS5000 series
Application	See Introduction, page 16-1
Frequency	As needed

Reference

Cisco Resource Pool Manager Server 1-1 Installation Guide

For all related documents, see [References, page 16-2](#).

Procedure

To correct the display of images on the Cisco RPMS GUI, perform the following steps:

-
- Step 1** Ensure that the following supported Web browsers are being used:
- Netscape 4.04 and higher
 - Microsoft Internet Explorer 4.x and higher
- If changing browsers solves the problem, the procedure is complete. Otherwise, proceed to Step 2.
- Step 2** Create a hosts file entry for the Cisco RPMS server on the client.
- On a UNIX client, create the hosts file entry in the following directory:
`/etc/hosts`
 - On Windows 2000 client, create the hosts file entry in the following directory:
`winnt\system32\drivers\etc\hosts`
- Step 3** If the images display correctly, the procedure is complete. Otherwise, contact the Cisco TAC for assistance.
-

Unable to Add/Change/Delete Administrators in the GUI

Description

Summary	Use this technique when you are unable to add, change, or delete administrators in the Cisco RPMS GUI.
Target Platform(s)	Cisco AS5000 series
Application	See Introduction, page 16-1
Frequency	As needed

Reference

Cisco Resource Pool Manager Server 1-1 Installation Guide

For all related documents, see [References, page 16-2](#).

Procedure

To add, change, or delete administrators in the RPMS GUI, perform the following steps:

Step 1 To do this, the Oracle data must be manipulated directly. Log in to the CLI as system root by using the following command:

```
su
cd <RPMS_home_dir>/bin./execsql "update cs_privilege set priv_value='\"ch3yQkFkeus8k\"'
where profile_id=(select profile_id from cs_user_profile where user_name='username')"
```

where

- *RPMS_home_dir*—is the home directory path for your Cisco RPMS system.
- *username*—is the user name of the root administrator.



Note The command listed above is entered on a single line.

This sets the password to *changeme*.

Step 2 Log in to the system and change the password for this administrator immediately.

RPMS Server Process Is Not Running

Description

Summary	Use this technique when the process for the Cisco RPMS server is not running.
Target Platform(s)	Cisco AS5000 series
Application	See Introduction, page 16-1
Frequency	As needed

Reference

Cisco Resource Pool Manager Server 1-1 Installation Guide

For all related documents, see [References, page 16-2](#).

Procedure

To restart the Cisco RPMS server process, perform the following steps:

-
- Step 1** Check the log files to determine a possible cause of the process failure by entering the following command:

```
tail <RPMS_home_dir>/log/rpmserver.log
tail <RPMS_home_dir>/log/rpms.log
```

where *RPMS_home_dir* is the home directory of your RPMS server.

Correct the cause of failure as necessary.

- Step 2** Stop the Cisco RPMS server process by entering the following command:

```
<RPMS_home_dir>/sbin/crpms rpmserver stop
```

where *RPMS_home_dir* is the home directory of your Cisco RPMS server.

- Step 3** Restart the Cisco RPMS server process by entering the following command:

```
<RPMS_home_dir>/sbin/crpms rpmserver start
```

where *RPMS_home_dir* is the home directory of your Cisco RPMS server.

Notes

- *Related tasks:* [RPMS Database Server Process Is Not Running, page 16-17](#)

RPMS Database Server Process Is Not Running

Description

Summary	Use this technique when the process for the Cisco RPMS database server is not running.
Target Platform(s)	Cisco AS5000 series
Application	See Introduction, page 16-1
Frequency	As needed

Reference

[Cisco Resource Pool Manager Server 1-1 Installation Guide](#)

For all related documents, see [References, page 16-2](#).

Procedure

To restart the RPMS database server process, perform the following steps:

Step 1 Check the log files to determine a possible cause of the process failure by entering the following command:

```
tail <RPMS_home_dir>/log/dberror_date
tail <RPMS_home_dir>/log/dbserver.log
```

where

- *RPMS_home_dir*—is the home directory of your Cisco RPMS server.
- *date*—is the date of the creation of the file.

Correct the cause of failure as necessary.

Step 2 Stop the Cisco RPMS database server process by entering the following command:

```
<RPMS_home_dir>/sbin/crpms dbserver stop
```

where *RPMS_home_dir* is the home directory of your Cisco RPMS server.

Step 3 Restart the Cisco RPMS database server process by entering the following command:

```
<RPMS_home_dir>/sbin/crpms dbserver start
```

where *RPMS_home_dir* is the home directory of your Cisco RPMS server.

Notes

- *Related tasks:* [RPMS Server Process Is Not Running](#), page 16-16

RPMS Watchdog Process Is Not Running

Description

Summary	Use this technique when the Cisco RPMS watchdog process is not running.
Target Platform(s)	Cisco AS5000 series
Application	See Introduction, page 16-1
Frequency	As needed

Reference

Cisco Resource Pool Manager Server 1-1 Installation Guide

For all related documents, see [References, page 16-2](#).

Procedure

To restart the Cisco RPMS watchdog process, perform the following steps:

-
- Step 1** Check the log file to determine a possible cause of the process failure by entering the following command:
- ```
tail <RPMS_home_dir>/log/watchdog.log
```
- where *RPMS\_home\_dir* is the home directory of your Cisco RPMS server.
- Correct the cause of failure as necessary.
- Step 2** Stop the Cisco RPMS watchdog process by entering the following command:
- ```
<RPMS_home_dir>/sbin/crpms watchdog stop
```
- where *RPMS_home_dir* is the home directory of your Cisco RPMS server.
- Step 3** Restart the Cisco RPMS watchdog process by entering the following command:
- ```
<RPMS_home_dir>/sbin/crpms watchdog start
```
- where *RPMS\_home\_dir* is the home directory of your Cisco RPMS server.
-

# Incorrect Access Server and Cisco RPMS Keys

## Description

|                           |                                                                                                    |
|---------------------------|----------------------------------------------------------------------------------------------------|
| <b>Summary</b>            | Use this technique when the system is configured with incorrect access server and Cisco RPMS keys. |
| <b>Target Platform(s)</b> | Cisco AS5000 series                                                                                |
| <b>Application</b>        | See <a href="#">Introduction, page 16-1</a>                                                        |
| <b>Frequency</b>          | As needed                                                                                          |

## Reference

*Cisco Resource Pool Manager Server 1-1 Installation Guide*

For all related documents, see [References, page 16-2](#).

## Procedure

To correct the keys on the access server and the Cisco RPMS, perform the following steps:

---

**Step 1** Debug TACACS by using the following command:

```
debug tacacs
```

The system returns a response similar to the following:

```
Jul 21 18:46:18.275 PDT: TAC+: Using default tacacs server-group "RPMS" list.
Jul 21 18:46:18.275 PDT: TAC+: Opening TCP/IP to 172.19.50.101/49 timeout=5
Jul 21 18:46:18.279 PDT: TAC+: Opened TCP/IP handle 0x65CC25BC to 172.19.50.101/
49 using source 172.19.50.45
Jul 21 18:46:18.279 PDT: TAC+: 172.19.50.101 (733062386) AUTHOR/START queued
Jul 21 18:46:18.479 PDT: TAC+: (733062386) AUTHOR/START processed
Jul 21 18:46:18.479 PDT: TAC+: received bad AUTHOR packet: type = 0, expected 2
Jul 21 18:46:18.479 PDT: TAC+: Invalid AUTHOR/START packet (check keys).
Jul 21 18:46:18.479 PDT: TAC+: Closing TCP/IP 0x65CC25BC connection to 172.19.50
.101/49
```

**Step 2** Reenter the keys on the access server and the Cisco RPMS.

**Step 3** If the keys are now correct, the procedure is complete. Otherwise, contact the Cisco TAC for assistance.

---

## Notes

- *Related tasks:* [Cisco RPMS Cannot Identify Access Server, page 16-21](#)

# Cisco RPMS Cannot Identify Access Server

## Description

- Summary** Use this technique when the Cisco RPMS cannot identify an access server. This can be caused by the following:
- The access server may not be configured correctly on the Cisco RPMS.
  - The name server entry may not match the source IP address for the access server.

**Note**

This problem appears to be the same as a mismatched key issue.

- Target Platform(s)** Cisco AS5000 series
- Application** See [Introduction, page 16-1](#)
- Frequency** As needed

## Reference

*Cisco Resource Pool Manager Server 1-1 Installation Guide*

For all related documents, see [References, page 16-2](#).

## Procedure

To ensure that the Cisco RPMS can identify an access server, perform the following steps:

- Step 1** Debug TACACS by entering the following command:

```
debug tacacs
```

The system returns a response similar to the following:

```
Jul 21 18:46:18.275 PDT: TAC+: Using default tacacs server-group "RPMS" list.
Jul 21 18:46:18.275 PDT: TAC+: Opening TCP/IP to 172.19.50.101/49 timeout=5
Jul 21 18:46:18.279 PDT: TAC+: Opened TCP/IP handle 0x65CC25BC to 172.19.50.101/
49 using source 172.19.50.45
Jul 21 18:46:18.279 PDT: TAC+: 172.19.50.101 (733062386) AUTHOR/START queued
Jul 21 18:46:18.479 PDT: TAC+: (733062386) AUTHOR/START processed
Jul 21 18:46:18.479 PDT: TAC+: received bad AUTHOR packet: type = 0, expected 2
Jul 21 18:46:18.479 PDT: TAC+: Invalid AUTHOR/START packet (check keys).
Jul 21 18:46:18.479 PDT: TAC+: Closing TCP/IP 0x65CC25BC connection to 172.19.50
.101/49
```

- Step 2** Ensure that the associated access server is defined on the Cisco RPMS server.
- Step 3** Ensure that the access server hostname and IP address match the name server entry.

**Step 4** Define the source address on the access server by entering the following command:

```
ip tacacs source-interface FastEthernet0/1
```

**Step 5** If the Cisco RPMS can identify the access server, the procedure is complete. Otherwise, contact the Cisco TAC for assistance.

---

## Notes

- *Related tasks:* [Incorrect Access Server and Cisco RPMS Keys, page 16-20](#)

# TACACS+ Single Connection Is Configured

## Description

|                           |                                                                                                                                                                                                                                                                                   |
|---------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Summary</b>            | Use this technique when there are repeated attempts to connect to the Cisco RPMS. This occurs when the TACACS server has been configured with a single connection, by means of the following command:<br><br><code>tacacs-server host &lt;IP address&gt; single-connection</code> |
| <b>Target Platform(s)</b> | Cisco AS5000 series                                                                                                                                                                                                                                                               |
| <b>Application</b>        | See <a href="#">Introduction, page 16-1</a>                                                                                                                                                                                                                                       |
| <b>Frequency</b>          | As needed                                                                                                                                                                                                                                                                         |

## Reference

*Cisco Resource Pool Manager Server 1-1 Installation Guide*

For all related documents, see [References, page 16-2](#).

## Procedure

To remove the single connection for the TACACS server, perform the following steps:

---

**Step 1** Debug the TACACS server by entering the following command:

```
debug tacacs
```

The system returns a response similar to the following:

```
Jul 24 12:37:12.440 PDT: TAC+: Opening TCP/IP to 172.19.50.101/49 timeout=5
Jul 24 12:37:12.440 PDT: TAC+: Opened TCP/IP handle 0x65F6AB1C to 172.19.50.101/
49 using source 172.19.50.45
Jul 24 12:37:12.640 PDT: TAC+: Closing TCP/IP 0x65F6AB1C connection to 172.19.50
.101/49
Jul 24 12:37:12.640 PDT: TAC+: Opening TCP/IP to 172.19.50.101/49 timeout=5
Jul 24 12:37:12.640 PDT: TAC+: Opened TCP/IP handle 0x65F6AFB8 to 172.19.50.101/
49 using source 172.19.50.45
Jul 24 12:37:12.840 PDT: TAC+: Closing TCP/IP 0x65F6AFB8 connection to 172.19.50
.101/49
```

**Step 2** Remove the single connection configuration by entering the following commands:

```
no tacacs-server host <IP address> single-connection
tacacs-server host <IP address>
```

where *IP address* is the IP address of the TACACS server.

---

# Port Counts Are Out of Synchronization

## Description

|                           |                                                                                                                                                                                                                                                                                                                                                                                                                   |
|---------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Summary</b>            | Use this technique when the port counts between the access server and the Cisco RPMS are out of synchronization. This is caused by one or more of the following: <ul style="list-style-type: none"><li>• The number of active calls reported on the Cisco RPMS does not match the number of active calls on the gateway.</li><li>• Calls are initially reported on the Cisco RPMS but are then cleared.</li></ul> |
| <b>Target Platform(s)</b> | Cisco AS5000 series                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>Application</b>        | See <a href="#">Introduction, page 16-1</a>                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Frequency</b>          | As needed                                                                                                                                                                                                                                                                                                                                                                                                         |

## Reference

*[Cisco Resource Pool Manager Server 1-1 Installation Guide](#)*

For all related documents, see [References, page 16-2](#).

## Procedure

To resolve the port discrepancy between the access server and the Cisco RPMS, perform the following steps:

- 
- |               |                                                                                                                                                      |
|---------------|------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | Ensure that the associated access server is configured with the required <b>administration</b> command:<br><code>tacacs-server administration</code> |
| <b>Step 2</b> | If the port discrepancy is resolved, the procedure is complete. Otherwise, contact the Cisco TAC for assistance.                                     |
-

# Oracle Configuration Updates Are Not Reflected on Snapshot Site Cisco RPMS Server(s)

## Description

|                           |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|---------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Summary</b>            | Use this technique when a Cisco RPMS server(s) pointing to the snapshot (replication) Oracle database server does not have an up-to-date configuration. This is caused by one or more of the following: <ul style="list-style-type: none"><li>• Cache triggers are not defined.</li><li>• The master Oracle database server is not set to update snapshot sites.</li><li>• The replication interval has not yet been reached (and a manual update is not performed).</li><li>• The cache trigger interval has not yet been reached.</li></ul> |
| <b>Target Platform(s)</b> | Cisco AS5000 series                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>Application</b>        | See <a href="#">Introduction, page 16-1</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>Frequency</b>          | As needed                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |

## Reference

*Cisco Resource Pool Manager Server 1-1 Installation Guide*

For all related documents, see [References, page 16-2](#).

## Procedure

To ensure the successful replication of the Oracle database, perform the following steps:



### Warning

---

**Oracle replication should only be attempted by an Oracle DBA.**

---

### Step 1

If this is your first replication attempt, perform the following steps. Otherwise, proceed to Step 2.

- Ensure that the cache triggers defined on the Cisco RPMS are pointing to the snapshot server.
- Ensure that a unique user name is being used as the Oracle replication administration user name.
- Ensure that an Oracle master is set to update snapshot site(s) of changes.
- Ensure that the replication interval is reached.
- Ensure that the cache trigger interval is reached.

- Step 2** If replication was previously working to the snapshot server/Cisco RPMS, perform the following steps:
- Ensure that the replication interval is reached.
  - Ensure that the cache trigger interval is reached.
  - Verify that the replication data is being received.

**Step 3** Verify that replication data is being received on the snapshot site.

**Step 4** Verify that the Cisco RPMS tables exist, by entering the following commands:

```
cd <RPMS_home_dir>/bin
./execsql "select table_name from user_tables"
```

Where *RPMS\_home\_dir* is the home directory of your Cisco RPMS.

The tables should be listed and the last line should indicate that 32 tables exist:

```
Number of rows fetched = 32
```

**Step 5** Verify that replication data is received on the snapshot site.

**Step 6** Check the Cisco RPMS schema to determine what data is received, that is, to check all customer profiles received, by entering the following command:

```
./execsql "select customer_name from cs_customer"
```

Refer to Appendix E of the *Cisco Resource Pool Manager 1-1 Configuration Guide* for complete table structure information.

---



# Enabling a Cisco RPMS Debugging Session

## Description

|                           |                                                                        |
|---------------------------|------------------------------------------------------------------------|
| <b>Summary</b>            | Use this technique when you need to debug problems on your Cisco RPMS. |
| <b>Target Platform(s)</b> | Cisco AS5000 series                                                    |
| <b>Application</b>        | See <a href="#">Introduction, page 16-1</a>                            |
| <b>Frequency</b>          | As needed                                                              |

## Reference

*Cisco Resource Pool Manager Server 1-1 Installation Guide*

For all related documents, see [References, page 16-2](#).

## Procedure

To enable a debug session on your Cisco RPMS, perform the following steps:

- 
- Step 1** Clear the log file by using the following commands:
- ```
csh
echo > rpms.log
echo > dbserver.log
```
- Step 2** Enable debugging on required subsystems by performing the following steps:
- Select **Detailed** for the level of debugging.
 - Select **Minor** for the level of error logging.
 - Click the **Update** button to apply the options you have selected.
- Step 3** Debugs appear in *rpms.log* and *dbserver.log* files.
-

Disabling a Cisco RPMS Debugging Session

Description

Summary	Use this technique when you have completed a debugging operation.
Target Platform(s)	Cisco AS5000 series
Application	See Introduction, page 16-1
Frequency	As needed

Reference

Cisco Resource Pool Manager Server 1-1 Installation Guide

For all related documents, see [References, page 16-2](#).

Procedure

To disable a debugging session on the Cisco RPMS, perform the following steps:

-
- Step 1** Deselect debugging on subsystems by performing the following steps:
- Select **Basic** for the level of debugging.
 - Select **Severe** for the level of error logging.
 - Click the **Update** button to apply the options you have selected.
- Step 2** Disabling a debugging session should be done as soon as possible.
-

Using show Commands

Description

Summary	Use the following show commands when troubleshooting Cisco RPMS problems.
Target Platform(s)	Cisco AS5000 series
Application	See Introduction, page 16-1
Frequency	As needed

Reference

[Cisco Resource Pool Manager Server 1-1 Installation Guide](#)

For all related documents, see [References, page 16-2](#).

Commands

The following **show** commands are helpful in diagnosing problems on the Cisco RPMS:

- **show resource-pool resource**
- **show resource-pool resource *name***
- **show resource-pool queue statistics**
- **show resource-pool queue description**
- **show csm call-rate**
- **show tacacs**

Using debug Commands

Description

Summary	Used the following debug commands to troubleshoot Cisco RPMS problems.
Target Platform(s)	Cisco AS5000 series
Application	See Introduction, page 16-1
Frequency	As needed

Reference

[Cisco Resource Pool Manager Server 1-1 Installation Guide](#)

For all related documents, see [References, page 16-2](#).

Commands

The following debug commands are helpful in diagnosing problems on the Cisco RPMS:

- **debug resource-pool**
- **debug aaa authorization**
- **debug tacacs**



Maintaining and Troubleshooting Cisco WAN Switches

This chapter contains the following information:

- [Using the Voice Interworking Service Module, Release 3.0](#)
- [Maintaining the MGX Route Processor Module](#)
- [Using Cisco MGM, Release 2.0](#)
- [Using Cisco WAN Manager, Release 10.5](#)

Introduction

This chapter provides operations, maintenance, and troubleshooting tasks related to the Cisco MGX 8850, Voice Interworking Service Module (VISM), and MGX Route Processor Module (RPM) in the Cisco PSTN Gateway Solution.



Note

This chapter *applies only* to the Cisco PSTN Gateway Solution.

Target Platforms

The following platforms are addressed in this chapter:

- VISM command line interface (CLI)
- Cisco MGM
- Cisco WAN Manager (CWM)

References

Cisco VISM 3.0 documentation can be found at the following URL:

<http://www.cisco.com/univercd/cc/td/doc/product/wanbu/mgx8850/vism30/index.htm>

Cisco MGM documentation can be found at the following URL:

<http://www.cisco.com/univercd/cc/td/doc/product/wanbu/cmgm/userguid/index.htm>

Cisco WAN Manager Release 10.5 documentation can be found at the following URL:

<http://www.cisco.com/univercd/cc/td/doc/product/wanbu/svplus/105/index.htm>

Using the Voice Interworking Service Module, Release 3.0

The VISM card, in combination with a Cisco MGX 8000 Series platform, enables telephone calls on conventional time-division multiplexed (TDM) voice circuits to be transported over an Asynchronous Transfer Mode (ATM) packet-switched and VoIP networks. The VISM card is a single height card designed to operate in the following platforms:

- Cisco MGX 8850 Release 1, wide area switch
- Cisco MGX 8250, edge concentrator
- Cisco MGX 8230, edge concentrator

For additional details, view the VISM 3.0 user documentation:

- <http://www.cisco.com/univercd/cc/td/doc/product/wanbu/mgx8850/vism30/index.htm>

Configuring VISM Features

The command line interface (CLI) is a DOS-like interface used to configure VISM cards. This chapter describes the following:

- Using the Command Line Interface
- Connecting to Cisco MGX 8000 Series Platforms
- Configuring VISM Features

For additional details, view the VISM 3.0 user documentation:

http://www.cisco.com/univercd/cc/td/doc/product/wanbu/mgx8850/vism30/vm30_04.htm

VISM CLI Commands

CLI commands allow you to configure, manage, and troubleshoot VISM to enable your applications. The VISM CLI commands are described in the remainder of this section and are arranged in alphabetical order.

For additional details, view the Voice Interworking Service Module, Release 3.0 user documentation:

http://www.cisco.com/univercd/cc/td/doc/product/wanbu/mgx8850/vism30/vm30_05.htm

Troubleshooting VISM

Use the following troubleshooting tools and techniques to assist you in maintaining your VISM card:

- VISM Card LEDs
- VISM and PXM Display, Log, and Diagnostic Loopback Path CLI Commands
- VISM Alarms
- UNIX Snoop Trace Tool

- Symptoms and Solutions

For additional details, view the Voice Interworking Service Module, Release 3.0 user documentation:

http://www.cisco.com/univercd/cc/td/doc/product/wanbu/mgx8850/vism30/vm30_06.htm

Maintaining the MGX Route Processor Module

This section describes maintenance procedures you might need to perform as your internetworking needs change.

Recovering a Lost Password

Following is an overview of the steps in the password recovery procedure:

- Virtual Configuration Register Settings
- Copying a Cisco IOS Image to Flash Memory

For additional details, view the RPM user documentation:

<http://www.cisco.com/univercd/cc/td/doc/product/wanbu/mgx8850/rpm/rpm14/appa.htm>

Using Cisco MGM, Release 2.0

This section provides an overview of the MGX Route Processor Module (RPM) and its relationship to the MGX 8230, MGX 8250, and MGX 8850 switch.

Cisco MGM User Interfaces

Cisco MGM provides a graphical user interface using UNIX Motif. For device specific configuration functions, Cisco MGM also provides access to the CiscoView GUI, as well as to command line interface functions through telnet sessions.

For detailed information on CiscoView, refer to the following documents:

- Overview for CiscoView
- CiscoView Getting Started Guide

For additional details, view the CMGM user documentation:

<http://www.cisco.com/univercd/cc/td/doc/product/wanbu/cmgm/userguid/orient.htm>

Cisco MGM Configuration

Cisco MGM automatically discovers network elements and displays them on the Map Viewer screen. From this screen you can view operational status and navigate to screens that support Cisco MGX 8000 Series Carrier Voice Gateway configuration and software upgrades.

For additional details, view the CMGM user documentation:

<http://www.cisco.com/univercd/cc/td/doc/product/wanbu/cmgm/userguid/manage.htm>

Cisco MGM Administration

Cisco MGM MapViewer displays information about Cisco MGX 8000 Series Carrier Voice Gateways, MGX 8000 Series components, and media gateway controllers (MGCs).

For additional details, view the CMGM user documentation:

<http://www.cisco.com/univercd/cc/td/doc/product/wanbu/cmgm/userguid/admin.htm>

Cisco MGM Fault and Performance Management

The Cisco MGM Alarm component, which is a customized component of the Cisco EMF platform, handles Cisco MGX 8000 Series Carrier Voice Gateway alarms and events. Cisco MGM receives alarm and event messages from managed objects and displays them in the MapViewer and Event Browser screens. MapViewer displays alarms on the topology view, and the event browser displays events in tabular form. The tabular data includes severity, date, source, and other information.

Cisco MGM implements alarm features using SNMP trap messages. A configuration file maps SNMP traps to Cisco MGM alarms. For more information, see the Cisco Element Management Framework User Guide.

Before Cisco MGM can process alarm information, you need to register the traps you want the Cisco MGX 8000 Series Carrier Voice Gateway to forward.

For additional details, view the CMGM user documentation:

<http://www.cisco.com/univercd/cc/td/doc/product/wanbu/cmgm/userguid/fault.htm>

Cisco MGM Security

Cisco MGM enforces security with user names and passwords, and manages user accounts individually and in groups. The use of access groups simplifies the process of assigning privileges to individual users because such groups enable you to define a set of privileges for each type of user.

For additional details, view the CMGM user documentation:

<http://www.cisco.com/univercd/cc/td/doc/product/wanbu/cmgm/userguid/secure.htm>

Using Cisco WAN Manager, Release 10.5

CWM, a suite of WAN multiservice management applications, provides powerful fault, configuration, and performance management functionality for WAN multiservice switches. CWM also provides robust statistics collection, storing the information in an Informix SQL database and allowing simple integration of this data into existing network management and operations systems.

Element and network management functions are provided by the CWM system, which can manage Cisco MGX 8230, Cisco MGX 8250, and both Release 1 and Release 2 Cisco MGX 8850 devices seamlessly.

**Note**

CWM supports additional hardware platforms not supported by the PSTN Gateway Solution.

CWM provides open interfaces for higher level service management systems.

The CWM desktop graphical user interface (GUI) provides the following applications that are found under the Apps pull down menu of the CWM Topology Main Window:

- Starting and Stopping Cisco WAN Manager
- Using Network Topology
- Connection Manager
- Network Browser
- Security Management
- Service Class Template Application
- Statistics Collection Manager
- Summary Reports and Wingz Report
- Network Configurator
- CWM to CWM Communications
- Downloading Software and Firmware
- Saving and Restoring Node Configurations
- Internet Connectivity
- Networking

For additional details, view Release 10.5 of the Cisco WAN Manager user documentation:

<http://www.cisco.com/univercd/cc/td/doc/product/wanbu/svplus/105/index.htm>



For terms or acronyms not listed below, see Internetworking Terms and Acronyms at the following URL:

<http://www.cisco.com/univercd/cc/td/doc/cisintwk/ita/index.htm>

A

AAA	authentication, authorization, and accounting
ALTDGK	alternate directory gatekeeper
AR	Cisco Access Registrar
ASAP	Cisco Any Service, Any Port solution
ASP	application service provider

B

BAMS	Cisco Billing and Measurements Server
-------------	---------------------------------------

C

CAC	call admission control
CBWFQ	class-based weighted fair queueing
CDR	call detail record
CHAP	Challenge Handshake Authentication Protocol
CIC	Cisco Info Center; carrier identification code
CLI	command line interface
CO	central office
CPU	central processing unit
CVM	CiscoWorks2000 Voice Manager

D

- DGK** directory gatekeeper
- DNIS** Dialed Number Identification Service

E

- EMEA** Europe, Middle East, and Africa
- EMS** element management system
- EO** end office

F

- FG** feature group

G

- GK** gatekeeper
- GW** gateway

H

- HDLC** high-level data link control
- HSRP** Hot Standby Router Protocol—used to ensure GK fault tolerance

I

ICMP	Internet Control Message Protocol
ICPIF	ITU G.113 Calculated Planning Impairment Factor
IETF	Internet Engineering Task Force
IMT	intermachine trunk
IPM	Cisco Internetwork Performance Monitor
IS	in service
ISP	Internet service provider
ISUP	ISDN User Part
ITSP	Internet telephony service provider
ITU	International Telecommunication Union
IVR	interactive voice response

L

L2F	Layer 2 Forwarding Protocol
L2TP	Layer 2 Tunneling Protocol
LFI	Cisco Link Fragmentation and Interleaving
LLQ	low latency queuing
LNS	L2TP network server

M

MGC	Media Gateway Controller
MGCP	Media Gateway Control Protocol
MIB	Management Information Base
MLP	Multilink PPP
MML	Man-Machine Language
MMP	Multichassis Multilink PPP
MTP	Message Transfer Part

N

NAS	network access server
NMS	network management system
NTP	Network Time Protocol
NFAS	Non-Facility Associated Signaling

O

OGW	originating gateway
OLO	other local operator; other licensed operator
OOS	out of service
OPC	origination point code
OPT	Open Packet Telephony
OSP	Open Settlements Protocol
OSS	Operations Support System

P

PCM	pulse code modulation
PDF	Portable Document Format
PIN	personal identification number
POP	point of presence
PPM	port policy management
PPP	Point-to-Point Protocol
PSQM	perceptual speech quality measure
PSTN	public switched telephone network
PTT	Post, Telephone, Telegraph—a government-mandated or -operated national telephony carrier

Q

QoS	quality of service
QoV	quality of voice (SNMP)

R

RADIUS	Remote Authentication Dial-In User Service
RAI	resource availability indicator
RAS	H.225 Registration, Admission, and Status Protocol—spoken between H.323 gateways and their gatekeepers
RLM	Cisco Redundant Link Manager
RPM	resource pool management; resource pool manager
RPMS	Cisco Resource Pool Manager Server
RSVP	Resource Reservation Protocol
RTCP	Real Time Conferencing Protocol; RTP Control Protocol
RTP	Real-Time Transport Protocol
RTR	Real Time Reporter

S

SC	signaling controller—a Cisco SC2200 signaling gateway that converts SS7 to a backhauled NI-2 protocol to gateways; see also VSC and MGC
SGBP	Stack Group Bidding Protocol
SGCP	Simple Gateway Control Protocol
SLT	signaling link termination; Cisco Signaling Link Terminal—a Cisco 2611 machine capable of terminating SS7 at the MTP2 layer and backhauling MTP3 (and up) to the SC2200 or virtual switch controller (VSC)
SNMP	Simple Network Management Protocol
SPE	system processing engine
SS7	Signaling System 7

T

TAC	Technical Assistance Center
TACACS	Terminal Access Controller Access Control System
TCL	Tool Command Language
TDM	time-division multiplex; time-division multiplexing
TFTP	Trivial File Transfer Protocol
TGW	terminating gateway

U

UG	universal gateway
UGM	Cisco Universal Gateway Manager
URL	uniform resource locator

V

VPDN	virtual private data (or dial) network
VSA	vendor-specific attribute—a nonstandard attribute tag used by RADIUS. Cisco has defined many useful VSAs to enhance the gateway CDR format.
VSC	virtual switch controller—one of various Cisco machines capable of providing SS7 signaling conversion, and able to control gateways by means of MGCP; referred to as the SC in this document
VWIC	Voice/WAN interface card

W

WFQ	weighted fair queuing
WIC	WAN interface card



Symbols

.ini files (Cisco UGM) [4](#)

A

accounting [1](#)

accounting records [5](#)

Adding gatekeepers in CVM

 local zone [5](#)

 remote zone [6](#)

administration [13](#)

administrators

 unable to change (Cisco RPMS) [15](#)

Adobe Acrobat

 Reader [xxxv](#)

 using [xxxv](#)

alarms [15](#)

 CIC [9](#)

 Cisco MGC, retrieving all [5](#)

 Cisco MGC, using troubleshooting procedures [7](#)

 Cisco MNM [19,21](#)

 configuring and verifying [7](#)

alerts

 CIC [9](#)

AMA BAF [3](#)

archive extraction error (Cisco RPMS) [3,4](#)

aregcmd command [2,6,12,15](#)

aregcmd command (Cisco AR) [6](#)

aregcmd commands [16](#)

arservagt command [11](#)

arstatus command (Cisco AR) [11](#)

asynchronous shell connections

 testing [6](#)

atdt (at) command [6](#)

attributes (Cisco AR) [5](#)

autodiscovery (Cisco UGM) [3](#)

B

BAMS [7](#)

baseline

 network performance [15](#)

bearer channel troubleshooting

 resolving stuck CICs [24](#)

billing [1](#)

billing logic [3](#)

bouncing SS7 links (correcting) [11](#)

busyout command [8](#)

C

CAC [6](#)

 configuring thresholds [4](#)

call completions [5](#)

call performance [5](#)

call trace

 alternatives [31](#)

 performing [30](#)

Call Tracker [8](#)

calltracker enable command [9](#)

CAR [7](#)

cautions [xxxvi](#)

CDRs [2](#)

 not being generated [39](#)

CEMF [2,1](#)

- CIC 7
 - starting and stopping components manually 4
- CICs
 - querying 18
 - resetting 23
 - resolving stuck 24
 - state mismatch, resolving 19
 - unblocking 22
 - validating 20
- CIC View Builder 16
- Cisco.com xxxviii
- Cisco 2611 Signaling Link Terminal 15
- Cisco AR 1,5
 - checking server 11
- Cisco ASAP Solution
 - References 2
- Cisco BAMS 3
- CISCO-CALL-APPLICATION-MIB 11
- Cisco CallTracker 8
- CISCO-CAS-IF-MIB 11
- Cisco Catalyst switches 15
- CISCO-DIAL-CONTROL-MIB 11
- Cisco Feature Navigator 11
- Cisco Generic Dial Plan Manager 16
- Cisco Info Center
 - server 5
- Cisco Info Server 2
 - creating new 8
 - managing 10
 - starting and stopping 5
- Cisco IOS Debug Command Reference 13
- Cisco MCG 3
- CISCO-MEMORY-POOL-MIB
 - using to monitor memory 4
- Cisco MGC
 - calls fail 28
 - call trace, alternatives 31
 - CICs, resolving stuck 24
 - disk space, clearing 33
 - hosts, recovering from failure 35
 - platform troubleshooting procedures 3
 - switchover, recovering from failure 34
- Cisco MGC (SC) node
 - manual deployment 7
 - using seed file to deploy 6
- Cisco MNM 7,1
 - diagnostic tools 24
 - event messages 26
 - viewing information about network devices 22
- CISCO-MODEM-MGMT-MIB 11
- Cisco PGW 2200 3,4
- CISCO-POP-MGMT-MIB 11
- Cisco PSTN Gateway Solution
 - References 3
- Cisco RPMS 15,5
- Cisco RPMS reports 5
- Cisco SC2200
 - monitoring disk space 3
 - monitoring peak call rates 3
 - testing failover 4
- Cisco SC2200 node 15,3
- Cisco SC2200 Signaling Controller 1
- CISCO-SIP-UA-MIB 11
- Cisco SS7 Interconnect for Voice Gateways Solution
 - References 2
- Cisco UGM 7,1
 - autodiscovery 3
 - deployment 3
 - network objects 3
- CiscoView 16
- CISCO-VOICE-DIAL-CONTROL-MIB 11
- CISCO-VOICE-IF-MIB 11
- CISCO-VOICE-NUMBER-EXPANSION-MIB 11
- Cisco VSPT 1
 - provisioning Cisco BAMS 4
- clear spe command 8
- Clients object (Cisco AR) 4
- clocking

- configuring and verifying [6](#)
- configuration and image management (Cisco UGM) [6](#)
- Configuration Manager (CIC) [6](#)
- Configure Administrative State function (Cisco UGM) [9](#)
- configuring devices with Cisco UGM [6](#)
- connection rates and speeds [6](#)
- controller logging (Cisco UGM) [3](#)
- controllers [6](#)
 - verifying [5](#)
- COT [6](#)
 - manual test [25](#)
 - settings, verifying [26](#)
- CPU load and memory use [5,6](#)
- CPU utilization [3](#)
- creating universal gateway groups in CVM [3](#)
- CVM [7,1](#)

D

- daemons (on Cisco SC2200 host) [5](#)
- data
 - inventory [4](#)
- database connectivity failure (Cisco RPMS) [7](#)
- database initialization failure (Cisco RPMS) [5](#)
- database server not running (Cisco RPMS) [17](#)
- data export [4](#)
- debug aaa authorization command [30](#)
- debug commands [13](#)
- debugging (Cisco RPMS) [24,27](#)
- debug resource-pool command [30](#)
- debug tacacs command [30](#)
- diagnostic tools
 - Cisco MNM [24](#)
- DIAL-CONTROL-MIB [11](#)
- dial plan
 - local [11](#)
 - local (POTS) [11](#)
 - network (VoIP) [12](#)
- discovery [13](#)

- Cisco MNM [9](#)
- discovery and deployment (Cisco UGM) [5](#)
- documentation
 - conventions [xxxv](#)
 - meaning of cautions [xxxvi](#)
 - meaning of notes [xxxvi](#)
 - meaning of timesavers [xxxvi](#)
 - meaning of tips [xxxvi](#)
 - release of [xxx](#)

E

- error messages [13](#)
- events [15](#)
 - CEMF, Cisco MNM, UGM [1](#)
 - CIC [9](#)
 - Cisco MNM [17,19,21](#)
 - messages in Cisco MNM [26](#)
- export [13](#)
- export (data) [4](#)
- exporting inventory data [4](#)

F

- facility-alarm command [7](#)
- failover
 - Cisco SC2200 [4](#)
- fault management (Cisco UGM) [7](#)
- faults, alarms, and traps
 - managing [10](#)
- Filter Builder (CIC) [15](#)
- filters (CIC) [14,15](#)
- firmware location command option [8](#)
- firmware upgrade command option [8](#)
- FXO [13](#)

G

- gatekeepers

- adding in CVM 4
- creating local clusters 9
- endpoints 10
- load balancing 9
- managing 11
- managing with IOS 9
- remote clusters 9
- verifying configuration 10

gateways

- using CallTracker to manage 8

general operations and maintenance guidelines (table) 5

GR-1100 3

GR-508 3

groups (Cisco AR) 7

GUI display problem (Cisco RPMS) 14

H

H.323

- start/stop records 2

H.323 gatekeepers 4

high availability 1

historyCriteria files (Cisco UGM) 4

I

ifconfig -a command 5

images

- managing 8
- using Cisco MNM to manage 10

interfaces file (CIC) 12

Internetworking Troubleshooting Handbook 17

inventory 4

IOS 7

IOS operations (Cisco UGM) 10

IP link

- media gateway, restoring 27

ISDN

- D-channels, resolving discrepancies in 21

- verifying PRI 5

ISDN D-channels (verifying) 6

K

keys (incorrect) (Cisco RPMS) 20

L

LDAP server 9

legend (application abbreviations) 7

load balancing 9

local cluster 9

local zone 5

log files (Cisco UGM) 4

logs

- Cisco MGC, viewing 6

M

major sections of the Cisco MGC Software Release 7 and Release 9 Operations, Maintenance, and Troubleshooting Guides (table) 2

management

- faults, alarms, and traps 10
- gatekeepers 11
- MIBs 14
- reports and data 12
- resources 9
- SS7 networks 12
- subscribers and ports 9

management applications for Cisco solutions (table) 16

Management Applications to Cisco Solution Components 17

management applications to Cisco solution components (figure) 17

Management Tools 15

Managing Dial Plans 2

Managing Network Elements 2

managing Voice Ports 2

- Master Process Control Server (CIC) 7
 - mcshadow utility 17
 - measurements
 - not being generated 38
 - operational 4
 - MGC 15
 - MIB
 - CISCO-CALL-APPLICATION-MIB 11
 - CISCO-CAS-IF-MIB 11
 - CISCO-DIAL-CONTROL-MIB 11
 - CISCO-MEMORY-POOL-MIB 4
 - CISCO-MODEM-MGMT-MIB 11
 - CISCO-POP-MGMT-MIB 11
 - CISCO-SIP-UA-MIB 11
 - CISCO-VOICE-DIAL-CONTROL-MIB 11
 - CISCO-VOICE-IF-MIB 11
 - CISCO-VOICE-NUMBER-EXPANSION-MIB 11
 - DIAL-CONTROL-MIB 11
 - MIB Locator 11
 - MIB objects in CISCO-MEMORY-POOL-MIB for monitoring show memory output 12
 - MIB objects in OLD-CISCO-CPU-MIB for monitoring CPU utilization (table) 12
 - MIBs
 - managing 14
 - managing objects 12
 - MICA modem commands 10
 - modem call completion 6
 - modem recovery command series 10
 - modems
 - managing 10
 - MTP timers
 - modifying 16
 - verifying 15
-
- N**
- nasmonitor command 18
 - nco_config configuration utility 12
 - nco_xigen utility 12
 - figures
 - Relationship of Resource and Element 17
 - relationship of resource and element 17
 - network management 8, 15
 - network management applications for the Cisco solutions (table) 16
 - network objects (in Cisco UGM) 3
 - network performance
 - monitoring with IOS 3
 - networks
 - managing 8
 - NextPort SPE commands 10
 - notes xxxvi
 - NTP 2
 - number normalization 11
-
- O**
- objects (CIC) 13
 - OLD-CISCO-CPU-MIB
 - using to monitor CPU load 3
 - operational measurements 4
 - Oracle database
 - failure to update 25
 - starting and stopping (Cisco RPMS) 10
-
- P**
- PDF xxxv
 - performance
 - Cisco MNM 13
 - monitoring 8
 - performance management (Cisco UGM) 8
 - physical layer failures
 - resolving 10
 - ping failure (Cisco UGM) 9
 - platform troubleshooting
 - CDRs, not being generated 39

- measurements, not being generated [38](#)
- peer, resolving failed connection to [41](#)
- properties, rebooting to modify [40](#)
- replication, verifying configuration [37](#)
- stored configuration data, restoring [36](#)
- polling [13](#)
 - Cisco MNM [11](#)
- port counts out of synchronizaion (Cisco RPMS) [24](#)
- ports
 - managing [9,7](#)
- Preface
 - Document Organization [2](#)
- Process Control (CIC) [7](#)
- Process Control Agents (CIC) [7](#)
- Profiles object [5](#)
- properties
 - rebooting to modify [40](#)
- ps -ef -o user,pid,pcpu -o args command [5](#)

R

- radclient command [2](#)
- radclient command (Cisco AR) [6](#)
- RADIUS proxy [1](#)
- RADIUS statistics [6](#)
- redundancy [1](#)
- References
 - Cisco ASAP Solution [2](#)
 - Cisco PSTN Gateway Solution [3](#)
 - Cisco SS7 Interconnect for Voice Gateways Solution [2](#)
- regularly scheduled operations and maintenance tasks (table) [3](#)
- rejected requests [5](#)
- release
 - of document [xxx](#)
 - of solution [xxx](#)
- remote clusters [9](#)
- remote processes [7](#)
- RemoteServer (Cisco AR) [9](#)

- remote zone [6](#)
- replication
 - configuration, verifying [37](#)
- reports
 - Cisco UGM [4](#)
- reports and data
 - management [12](#)
- resource management [14](#)
- resources
 - managing [9](#)
- RLM
 - restoring [27](#)
 - timers, modifying [29](#)
- RPMS [7](#)
- rtrv-alm::cont command [5](#)
- rtrv-ctr command [5](#)
- rtrv-ne command [5](#)
- rtrv-ne-health::all command [5](#)
- rtrv-softw::all command [5](#)

S

- scheduling [8](#)
- scheduling tasks
 - in CVM [10](#)
- security [12](#)
 - Cisco MNM [5](#)
 - user access (CIC) [14](#)
- seed file [6](#)
- server not running (Cisco RPMS) [16](#)
- server triggers [9](#)
- session management [10](#)
- Session Manager (Cisco AR) [10](#)
- show async status command [5](#)
- show call calltracker summary command [9](#)
- show caller command [6](#)
- show call spike status command [5](#)
- show call threshold command [5](#)
- show call treatment command [5](#)

- show controller command 5
- show controller t3 command 5
- show csm call-rate command 29
- show gatekeeper command 10
- show interface async 4/0 command 5
- show interface serial command 6
- show isdn service command 5
- show isdn status command 5
- show line command 6
- show memory command 3
- show port command 7
- show process command 5
- show processes command 3
- show resource-pool queue description command 29
- show resource-pool queue statistics command 29
- show resource-pool resource command 29
- show resource-pool resource name command 29
- show running-config command 5
- show spe command 6,7
- show spe digital command 7
- show spe modem command 7
- show spe voice command 7
- show tacacs command 29
- show tdm clocks command 7
- show user command 6
- shutdown command 8
- SLAs 14
- SNMP 15
- spe download maintenance command 8
- SPE performance
 - managing and viewing statistics 7
- spe recovery command 8
- spe recovery command series 10
- SPEs
 - managing and troubleshooting 8
 - upgrading firmware 8
- SS7
 - deploying network 6
- SS7 dial plan

- verifying proper loading 17
- SS7 DPC
 - restoring 14
 - service, restoring 12
- SS7 links
 - bouncing, correcting 11
 - service, restoring 8
- SS7 loadsharing
 - malfunction, resolving 9
- SS7 network
 - configuring devices for management 4
 - deployment 7
 - discovery 9
 - managing signaling components 1
 - performance 13
 - polling 11
- SS7 networks
 - managing 12
- SS7 route
 - restoring 13
- start/stop records 2
- start packet 5
- stop packet 5
- subscribers
 - managing 9
- synchronization 8
- synchronization (GWs and GKs) 9
- synchronizing devices in CVM 8
- syslog daemon 13

T

- tables
 - General Operations and Maintenance Guidelines 5
 - Major Sections of the Cisco MGC Software Release 7 and Release 9 Operations, Maintenance, and Troubleshooting Guide 2
 - Management Applications for Cisco Solutions 16
 - MIB Objects in CISCO-MEMORY-POOL-MIB for Monitoring Show Memory Output 12

MIB Objects in OLD-CISCO-CPU-MIB for Monitoring CPU Utilization [12](#)

Network Management Applications for the Cisco Solutions [16](#)

Regularly Scheduled Operations and Maintenance Tasks [3](#)

Tasks for Configuring Call Admission Control Thresholds [4](#)

Useful Cisco MIBs that Support the Cisco ASAP Solution [11](#)

TAC (Technical Assistance Center) [xxxviii](#)

tasks for configuring Call Admission Control thresholds (table) [4](#)

TCAP trace

- Cisco MGC [32](#)

thresholds [15](#)

timeouts [5](#)

timesavers [xxxvi](#)

timestamps [2](#)

tips [xxxvi](#)

TLV [3](#)

TNS Listener [8](#)

- starting and stopping (Cisco RPMS) [12](#)

traffic patterns [3](#)

traps

- Cisco MNM [15, 17, 19, 21](#)

triggers [9](#)

troubleshooting

- configuration and image management (Cisco UGM) [6](#)
- Configure Administrative State function (Cisco UGM) [9](#)
- discovery and deployment (Cisco UGM) [5](#)
- fault management (Cisco UGM) [7](#)
- Internetworking Troubleshooting Handbook [17](#)
- IOS operations (Cisco UGM) [10](#)
- performance management (Cisco UGM) [8](#)
- ping failure (Cisco UGM) [9](#)
- platform procedures [3](#)
- polling (Cisco UGM) [8](#)

U

UG group [3](#)

universal port card and lines

- verifying [6](#)

upgrades

- billing components [2](#)
- network management applications [2](#)

URL [xxxv](#)

useful Cisco MIBs that support the Cisco ASAP Solution (table) [11](#)

UserList (Cisco AR) [8](#)

V

views [16](#)

vmstat command [5](#)

voice ports

- FXO, FXS, E&M, ISDN [13](#)

VSPT [7](#)

W

watchdog process not running (Cisco RPMS) [19](#)

Weblink Preferences [xxxv](#)

Web server fails to start (Cisco RPMS) [9](#)

Z

zone

- local [5](#)
- logical [3](#)
- remote [6](#)

