



Cisco BTS 10200 Softswitch Troubleshooting Guide, Release 4.4

Revised: October 23, 2008

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.

Americas 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: 408 527-0883

Text Part Number: OL-11335-06

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.

CCDE, CCENT, Cisco Eos, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, Cisco TelePresence, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website 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. (0807R)

Cisco BTS 10200 Softswitch Troubleshooting Guide, Release 4.4
Copyright © 2008 Cisco Systems, Inc. All rights reserved.



CONTENTS

Preface xxxv

Introduction	xxxv
Objective	xxxv
Audience	xxxv
Organization	xxxvi
Conventions	xxxvii
Updates to this Document for Release 4.4	xxxvii
Obtaining Documentation	xxxvii
Cisco.com	xxxvii
Documentation CD-ROM	xxxviii
Ordering Documentation	xxxviii
Documentation Feedback	xxxviii
Obtaining Technical Assistance	xxxviii
Cisco TAC Website	xxxix
Opening a TAC Case	xxxix
TAC Case Priority Definitions	xxxix
Obtaining Additional Publications and Information	xl

CHAPTER 1

Troubleshooting Overview 1-1

Introduction	1-1
Interoperability	1-1
Symptoms, Problems, and Solutions	1-2
General Problem-Solving Model	1-2
Resolving Network Problems	1-4
Resolving System Problems	1-5
Managing Events and Alarms	1-8
Managing Event and Alarm Reports	1-9
Show Alarm Command	1-9
Report Alarm Command	1-10
Ack Alarm Command	1-11
Clear Alarm Command	1-11
Format of Alarm Reports	1-12
Events and Alarm Logs	1-13

Viewing Event or Alarm Logs	1-13
Show, Add, and Delete Event Queue Commands	1-15
Saving Events to Log Files	1-15
Show Report-Properties Command	1-15
Changing Report Properties	1-15
Changing Threshold and Throttle Values	1-16
Managing and Responding to Events and Alarms	1-17
Events and Alarms Descriptions and Corrective Actions	1-18
Format of Events and Alarms	1-18

CHAPTER 2

Audit Troubleshooting 2-1

Introduction	2-1
Audit Events and Alarms	2-2
AUDIT (1)	2-2
AUDIT (2)	2-2
AUDIT (3)	2-3
AUDIT (4)	2-3
AUDIT (5)	2-4
AUDIT (6)	2-4
AUDIT (7)	2-5
AUDIT (8)	2-5
Monitoring Audit Events	2-6
Test Report - Audit (1)	2-6
Start or Stop of Signaling System 7 - Circuit Identification Code Audit - Audit (2)	2-6
Signaling System 7 Circuit Identification Code Audit Terminated Before Successful Completion - Audit (3)	2-6
Call Exceeds a Long-Duration Threshold - Audit (4)	2-7
Critical Internal Audit Failure - Audit (5)	2-7
Major Internal Audit Failure - Audit (6)	2-7
Minor Internal Audit Failure - Audit (7)	2-7
Warning From Internal Audit - Audit (8)	2-8
Troubleshooting Audit Alarms	2-9
Critical Internal Audit Failure - Audit (5)	2-9
Major Internal Audit Failure - Audit (6)	2-9
Minor Internal Audit Failure - Audit (7)	2-9

CHAPTER 3

Billing Troubleshooting 3-1

Introduction	3-1
Billing Events and Alarms	3-2

BILLING (1)	3-2
BILLING (2)	3-3
BILLING (3)	3-4
BILLING (4)	3-5
BILLING (5)	3-5
BILLING (6)	3-6
BILLING (7)	3-7
BILLING (8)	3-7
BILLING (13)	3-8
BILLING (14)	3-8
BILLING (15)	3-9
BILLING (29)	3-9
BILLING (30)	3-10
BILLING (31)	3-10
BILLING (32)	3-10
BILLING (33)	3-11
BILLING (35)	3-11
BILLING (36)	3-12
BILLING (37)	3-12
BILLING (38)	3-13
BILLING (39)	3-13
BILLING (40)	3-14
BILLING (41)	3-14
BILLING (42)	3-15
BILLING (44)	3-15
BILLING (45)	3-16
BILLING (46)	3-16
BILLING (47)	3-17
BILLING (48)	3-17
BILLING (49)	3-18
BILLING (52)	3-18
BILLING (53)	3-19
BILLING (54)	3-19
BILLING (55)	3-20
BILLING (56)	3-20
BILLING (57)	3-21
BILLING (58)	3-21
Monitoring Billing Events	3-22
Test Report - Billing (1)	3-23
Billing Partition Disk Usage Minor Threshold Exceeded - Billing (2)	3-23

Billing Partition Disk Usage Major Threshold Exceeded - Billing (3)	3-23
Billing Partition Disk Usage Critical Threshold Exceeded - Billing (4)	3-23
Billing Partition Disk Usage Within Normal Range - Billing (5)	3-23
File Transfer Protocol/Secure File Transfer Protocol Transfer Failed - Billing (6)	3-24
Transmission Control Protocol Connection Error - Billing (7)	3-24
Transmission Control Protocol Packet Receive Failure - Billing (8)	3-24
Database Connection Error - Billing (13)	3-24
File Open Error - Billing (14)	3-24
File Write Error - Billing (15)	3-24
Call Data Block Send Failed - Billing (29)	3-25
Domain Name Mapping Failed - Billing (30)	3-25
Port not Specified - Billing (31)	3-25
Element Management System Address not Specified - Billing (32)	3-25
File Transfer Protocol/Secure File Transfer Protocol Parameters Invalid - Billing (33)	3-25
All Billing Links at Billing Server Down - Billing (35)	3-25
Billing Link Restored - Billing (36)	3-26
Billing Link Failure - Billing (37)	3-26
Event Message Log File Access Error - Billing (38)	3-26
RADIUS Accounting Receive Failure - Billing (39)	3-26
Event Message Encode Failure - Billing (40)	3-26
Message Content Error - Billing (41)	3-26
Error Reading Provisioned Data—Using Default - Billing (42)	3-26
Record Keeping System Switch Occurred - Billing (44)	3-27
Event Message Log File Opened - Billing (45)	3-27
Event Message Log File Closed - Billing (46)	3-27
Record Keeping System Unreachable for One Hour - Billing (47)	3-27
Record Keeping System Unreachable for Three Hours - Billing (48)	3-27
Record Keeping System Unreachable for Five Hours - Billing (49)	3-27
Bulk Data Management System Stopped Generating New Billing File - Billing (52)	3-28
Event Message Disk Space 50 Percent Full - Billing (53)	3-28
Event Message Disk Space 70 Percent Full - Billing (54)	3-28
Event Message Disk Space 100 Percent Full - Billing (55)	3-28
Billing Data Corruption Detected - Billing (56)	3-28
Prepaid Subscriber Call Attempt Failed Because of Balance - Billing (57)	3-28
Signaling Prepaid Server Inaccessible - Billing (58)	3-29
Troubleshooting Billing Alarms	3-30
Billing Partition Disk Usage Minor Threshold Exceeded - Billing (2)	3-31
Billing Partition Disk Usage Major Threshold Exceeded - Billing (3)	3-31
Billing Partition Disk Usage Critical Threshold Exceeded - Billing (4)	3-31
File Transfer Protocol/Secure File Transfer Protocol Transfer Failed - Billing (6)	3-32

Transmission Control Protocol Connection Error - Billing (7)	3-33
Transmission Control Protocol Packet Receive Failure - Billing (8)	3-33
Database Connection Error - Billing (13)	3-33
File Write Error - Billing (15)	3-33
Call Data Block Send Failed - Billing (29)	3-33
Domain Name Mapping Failed - Billing (30)	3-34
Port not Specified - Billing (31)	3-34
Element Management System Address not Specified - Billing (32)	3-34
File Transfer Protocol/Secure File Transfer Protocol Parameters Invalid - Billing (33)	3-34
All Billing Links at Billing Server Down - Billing (35)	3-34
Billing Link Failure - Billing (37)	3-35
Event Message Log File Access Error - Billing (38)	3-35
RADIUS Accounting Receive Failure - Billing (39)	3-35
Event Message Encode Failure - Billing (40)	3-35
Message Content Error - Billing (41)	3-35
Record Keeping System Switch Occurred - Billing (44)	3-36
Event Message Log File Opened - Billing (45)	3-36
Event Message Log File Closed - Billing (46)	3-36
Record Keeping System Unreachable for One Hour - Billing (47)	3-36
Record Keeping System Unreachable for Three Hours - Billing (48)	3-36
Record Keeping System Unreachable for 5 Hours - Billing (49)	3-37
Bulk Data Management System Stopped Generating New Billing File - Billing (52)	3-37
Event Message Disk Space 50 Percent Full - Billing (53)	3-37
Event Message Disk Space 70 Percent Full - Billing (54)	3-37
Event Message Disk Space 100 Percent Full - Billing (55)	3-37
Billing Data Corruption Detected - Billing (56)	3-38
Signaling Prepaid Server Inaccessible - Billing (58)	3-38

CHAPTER 4

Call Processing Troubleshooting 4-1

Introduction	4-1
Call Processing Events and Alarms	4-2
CALLP (1)	4-3
CALLP (8)	4-3
CALLP (9)	4-4
CALLP (11)	4-4
CALLP (12)	4-5
CALLP (13)	4-5
CALLP (14)	4-6
CALLP (15)	4-6

CALLP (16)	4-7
CALLP (17)	4-7
CALLP (18)	4-8
CALLP (19)	4-8
CALLP (20)	4-9
CALLP (21)	4-9
CALLP (22)	4-10
CALLP (23)	4-10
CALLP (24)	4-11
CALLP (25)	4-11
CALLP (26)	4-12
CALLP (27)	4-12
CALLP (28)	4-13
CALLP (29)	4-13
CALLP (30)	4-14
CALLP (31)	4-14
CALLP (32)	4-15
CALLP (33)	4-15
CALLP (34)	4-16
CALLP (35)	4-16
CALLP (36)	4-17
CALLP (37)	4-17
CALLP (38)	4-18
CALLP (39)	4-18
Monitoring Call Processing Events	4-19
Test Report - Call Processing (1)	4-20
No Route Available for Called Number - Call Processing (8)	4-20
No Route Available for Carrier Dialed - Call Processing (9)	4-20
Feature Server One Link Down - Call Processing (11)	4-20
Feature Server Both Links Down - Call Processing (12)	4-21
Network Access Server Create Connection Error - Call Processing (13)	4-21
Network Access Server Authentication Failure - Call Processing (14)	4-21
Cable Modem Termination System Easily Recognizable Identification Not Found in Media Gateway Table - Call Processing (15)	4-21
Route Index has No Trunk Group Assigned - Call Processing (16)	4-21
Invalid Route Index Used - Call Processing (17)	4-21
Unable to Play Announcement - Call Processing (18)	4-22
Call Routed to Unprovisioned Subscriber - Call Processing (19)	4-22
No Route or Trunk Group Available to Route Call - Call Processing (20)	4-22
Call Released Due to Maximum Hop Counts Exceeded - Call Processing (21)	4-22

Trunk Group Index Read Failure - Call Processing (22)	4-22
Routing Error: Termination is Not a Subscriber - Call Processing (23)	4-22
Invalid Route for Subscriber Index - Call Processing (24)	4-23
Invalid Route Group for Subscriber Routing - Call Processing (25)	4-23
Invalid Trunk Group for Subscriber Routing - Call Processing (26)	4-23
Unable to Route: Blocked by Destination Subscriber Status - Call Processing (27)	4-23
Route Name Does Not Exist - Call Processing (28)	4-23
Routing Selection Failure - Call Processing (29)	4-23
Customer-Originated Trace Test Failed - Call Processing (30)	4-24
Call Authorization Failure - Call Processing (31)	4-24
Country Code Dialing Plan Error - Call Processing (32)	4-24
Invalid Call - Call Processing (33)	4-24
Dial Plan Information Not Found for Digits Received - Call Processing (34)	4-24
Dial Plan Information for Test Call Not Found - Call Processing (35)	4-24
Invalid or Unknown Nature of Address - Call Processing (36)	4-25
Call Failure - Call Processing (37)	4-25
Release Cause 25 Exchange Routing Error Received - Call Processing (38)	4-25
Test Call Blocked Due to Congestion or Isolation - Call Processing (39)	4-25
Troubleshooting Call Processing Alarms	4-26
Feature Server One Link Down - Call Processing (11)	4-26
Feature Server Both Links Down - Call Processing (12)	4-28
Release Cause 25 Exchange Routing Error Received - Call Processing (38)	4-29

CHAPTER 5

Configuration Troubleshooting 5-1

Introduction	5-1
Configuration Events and Alarms	5-2
CONFIG (1)	5-2
CONFIG (2)	5-2
CONFIG (3)	5-3
CONFIG (4)	5-3
Monitoring Configuration Events	5-4
Test Report - Configuration (1)	5-4
Signaling Media Gateway Adapter Wrongly Configured Domain Name - Configuration (2)	5-4
Mate Configuration Error - Configuration (3)	5-4
Configuration Error - Configuration (4)	5-4
Troubleshooting Configuration Alarms	5-5
Mate Configuration Error - Configuration (3)	5-5
Configuration Error - Configuration (4)	5-5

CHAPTER 6**Database Troubleshooting 6-1**

Introduction 6-1

Database Events and Alarms 6-2

DATABASE (1) 6-2

DATABASE (2) 6-3

DATABASE (3) 6-4

DATABASE (4) 6-5

DATABASE (5) 6-6

DATABASE (6) 6-6

DATABASE (7) 6-7

DATABASE (8) 6-8

DATABASE (9) 6-8

DATABASE (10) 6-9

DATABASE (11) 6-9

DATABASE (12) 6-10

DATABASE (13) 6-11

DATABASE (14) 6-11

DATABASE (15) 6-12

DATABASE (16) 6-12

DATABASE (17) 6-13

DATABASE (18) 6-13

DATABASE (19) 6-14

DATABASE (20) 6-14

Monitoring Database Events 6-15

Test Report - Database (1) 6-15

Database Management Update Failure: Master/Slave Database Out of Sync - Database (2) 6-16

There are Errors in Element Management System Database DefError Queue; Contact Database Administrator - Database (3) 6-16

Element Management System Database HeartBeat: Replication PUSH Job Broken - Database (4) 6-16

Element Management System Database HeartBeat Process Died - Database (5) 6-16

Element Management System Database Replication DefTranDest Queue Overloaded - Database (6) 6-16

Element Management System Database DefTran Queue is Overloaded - Database (7) 6-17

Element Management System Database Tablespace is Out of Free Space - Database (8) 6-17

Urgent: Element Management System Database Archive Log Directory is Getting Full - Database (9) 6-17

Element Management System Database: Backup Fails - Database (10) 6-17

Element Management System Database Alert.log Alerts - Database (11) 6-17

Element Management System Database Process Died - Database (12) 6-17

Element Management System Database Performance Alert - Database (13)	6-18
Table Size Exceeds Minor Threshold Limit - Database (14)	6-18
Table Size Exceeds Major Threshold Limit - Database (15)	6-18
Table Size Exceeds Critical Threshold Limit - Database (16)	6-18
Data Replication Failed - Database (17)	6-18
Unexpected Runtime Data Interaction - Database (18)	6-18
Daily Database Backup Completed Successfully - Database (19)	6-19
Replication Data Flush Timeout During Switchover - Database (20)	6-19
Troubleshooting Database Alarms	6-20
There Are Errors in Element Management System Database DefError Queue; Contact Database Administrator - Database (3)	6-21
Element Management System Database HeartBeat: Replication PUSH Job Broken - Database (4)	6-21
Element Management System Database HeartBeat Process Died - Database (5)	6-21
Element Management System Database Replication DefTranDest Queue Overloaded - Database (6)	6-22
Element Management System Database DefTran Queue is Overloaded - Database (7)	6-22
Element Management System Database Tablespace is Out of Free Space - Database (8)	6-22
Urgent: Element Management System Database Archive Log Directory is Getting Full - Database (9)	6-22
Element Management System Database: Backup Fails - Database (10)	6-22
Element Management System Database Alert.log Alerts - Database (11)	6-23
Element Management System Database Process Died - Database (12)	6-23
Element Management System Database Performance Alert - Database (13)	6-23
Table Size Exceeds Minor Threshold Limit - Database (14)	6-23
Table Size Exceeds Major Threshold Limit - Database (15)	6-24
Table Size Exceeds Critical Threshold Limit - Database (16)	6-24
Data Replication Failed - Database (17)	6-24
Replication Data Flush Timeout During Switchover - Database (20)	6-24

CHAPTER 7**Maintenance Troubleshooting 7-1**

Introduction	7-1
Maintenance Events and Alarms	7-2
MAINTENANCE (1)	7-3
MAINTENANCE (2)	7-3
MAINTENANCE (3)	7-4
MAINTENANCE (4)	7-5
MAINTENANCE (5)	7-6
MAINTENANCE (6)	7-7
MAINTENANCE (7)	7-8

MAINTENANCE (8)	7-9
MAINTENANCE (9)	7-9
MAINTENANCE (10)	7-10
MAINTENANCE (11)	7-10
MAINTENANCE (12)	7-11
MAINTENANCE (13)	7-11
MAINTENANCE (14)	7-12
MAINTENANCE (15)	7-12
MAINTENANCE (16)	7-13
MAINTENANCE (17)	7-13
MAINTENANCE (18)	7-14
MAINTENANCE (19)	7-14
MAINTENANCE (20)	7-15
MAINTENANCE (21)	7-15
MAINTENANCE (22)	7-16
MAINTENANCE (23)	7-16
MAINTENANCE (24)	7-17
MAINTENANCE (25)	7-17
MAINTENANCE (26)	7-18
MAINTENANCE (27)	7-18
MAINTENANCE (28)	7-18
MAINTENANCE (29)	7-19
MAINTENANCE (30)	7-19
MAINTENANCE (32)	7-20
MAINTENANCE (33)	7-20
MAINTENANCE (34)	7-21
MAINTENANCE (35)	7-21
MAINTENANCE (36)	7-22
MAINTENANCE (37)	7-22
MAINTENANCE (38)	7-23
MAINTENANCE (39)	7-23
MAINTENANCE (40)	7-23
MAINTENANCE (41)	7-24
MAINTENANCE (42)	7-24
MAINTENANCE (43)	7-25
MAINTENANCE (44)	7-25
MAINTENANCE (45)	7-26
MAINTENANCE (46)	7-26
MAINTENANCE (47)	7-27
MAINTENANCE (48)	7-27

MAINTENANCE (49)	7-28
MAINTENANCE (50)	7-29
MAINTENANCE (51)	7-29
MAINTENANCE (52)	7-30
MAINTENANCE (53)	7-30
MAINTENANCE (54)	7-31
MAINTENANCE (55)	7-31
MAINTENANCE (56)	7-32
MAINTENANCE (57)	7-32
MAINTENANCE (58)	7-33
MAINTENANCE (61)	7-34
MAINTENANCE (62)	7-34
MAINTENANCE (63)	7-35
MAINTENANCE (64)	7-35
MAINTENANCE (65)	7-36
MAINTENANCE (66)	7-36
MAINTENANCE (67)	7-37
MAINTENANCE (68)	7-37
MAINTENANCE (69)	7-38
MAINTENANCE (70)	7-38
MAINTENANCE (71)	7-39
MAINTENANCE (72)	7-39
MAINTENANCE (73)	7-40
MAINTENANCE (74)	7-40
MAINTENANCE (75)	7-41
MAINTENANCE (77)	7-41
MAINTENANCE (78)	7-42
MAINTENANCE (79)	7-42
MAINTENANCE (80)	7-43
MAINTENANCE (81)	7-43
MAINTENANCE (82)	7-44
MAINTENANCE (83)	7-44
MAINTENANCE (84)	7-45
MAINTENANCE (85)	7-45
MAINTENANCE (86)	7-46
MAINTENANCE (87)	7-46
MAINTENANCE (88)	7-47
MAINTENANCE (89)	7-47
MAINTENANCE (90)	7-48
MAINTENANCE (91)	7-48

MAINTENANCE (92)	7-49
MAINTENANCE (93)	7-49
MAINTENANCE (94)	7-50
MAINTENANCE (95)	7-50
MAINTENANCE (96)	7-51
MAINTENANCE (97)	7-51
MAINTENANCE (98)	7-52
MAINTENANCE (99)	7-52
MAINTENANCE (100)	7-53
MAINTENANCE (101)	7-53
MAINTENANCE (102)	7-54
MAINTENANCE (103)	7-54
Monitoring Maintenance Events	7-55
Test Report - Maintenance (1)	7-58
Report Threshold Exceeded - Maintenance (2)	7-58
Local Side has Become Faulty - Maintenance (3)	7-58
Mate Side has Become Faulty - Maintenance (4)	7-58
Changeover Failure - Maintenance (5)	7-58
Changeover Timeout - Maintenance (6)	7-59
Mate Rejected Changeover - Maintenance (7)	7-59
Mate Changeover Timeout - Maintenance (8)	7-59
Local Initialization Failure - Maintenance (9)	7-59
Local Initialization Timeout - Maintenance (10)	7-59
Switchover Complete - Maintenance (11)	7-59
Initialization Successful - Maintenance (12)	7-59
Administrative State Change - Maintenance (13)	7-60
Call Agent Administrative State Change - Maintenance (14)	7-60
Feature Server Administrative State Change - Maintenance (15)	7-60
Process Manager: Starting Process - Maintenance (16)	7-60
Invalid Event Report Received - Maintenance (17)	7-60
Process Manager: Process has Died - Maintenance (18)	7-60
Process Manager: Process Exceeded Restart Rate - Maintenance (19)	7-60
Lost Connection to Mate - Maintenance (20)	7-61
Network Interface Down - Maintenance (21)	7-61
Mate is Alive - Maintenance (22)	7-61
Process Manager: Process Failed to Complete Initialization - Maintenance (23)	7-61
Process Manager: Restarting Process - Maintenance (24)	7-61
Process Manager: Changing State - Maintenance (25)	7-61
Process Manager: Going Faulty - Maintenance (26)	7-61
Process Manager: Changing Over to Active - Maintenance (27)	7-62

Process Manager: Changing Over to Standby - Maintenance (28)	7-62
Administrative State Change Failure - Maintenance (29)	7-62
Element Manager State Change - Maintenance (30)	7-62
Process Manager: Sending Go Active to Process - Maintenance (32)	7-62
Process Manager: Sending Go Standby to Process - Maintenance (33)	7-62
Process Manager: Sending End Process to Process - Maintenance (34)	7-63
Process Manager: All Processes Completed Initialization - Maintenance (35)	7-63
Process Manager: Sending All Processes Initialization Complete to Process - Maintenance (36)	7-63
Process Manager: Killing Process - Maintenance (37)	7-63
Process Manager: Clearing the Database - Maintenance (38)	7-63
Process Manager: Cleared the Database - Maintenance (39)	7-63
Process Manager: Binary Does not Exist for Process - Maintenance (40)	7-64
Administrative State Change Successful with Warning - Maintenance (41)	7-64
Number of Heartbeat Messages Received is Less Than 50% of Expected - Maintenance (42)	7-64
Process Manager: Process Failed to Come Up in Active Mode - Maintenance (43)	7-64
Process Manager: Process Failed to Come Up in Standby Mode - Maintenance (44)	7-64
Application Instance State Change Failure - Maintenance (45)	7-64
Network Interface Restored - Maintenance (46)	7-65
Thread Watchdog Counter Expired for a Thread - Maintenance (47)	7-65
Index Table Usage Exceeded Minor Usage Threshold Level - Maintenance (48)	7-65
Index Table Usage Exceeded Major Usage Threshold Level - Maintenance (49)	7-65
Index Table Usage Exceeded Critical Usage Threshold Level - Maintenance (50)	7-65
A Process Exceeds 70% of Central Processing Unit Usage - Maintenance (51)	7-65
Central Processing Unit Usage is Now Below the 50% Level - Maintenance (52)	7-66
The Central Processing Unit Usage is Over 90% Busy - Maintenance (53)	7-66
The Central Processing Unit has Returned to Normal Levels of Operation - Maintenance (54)	7-66
The Five Minute Load Average is Abnormally High - Maintenance (55)	7-66
The Load Average has Returned to Normal Levels - Maintenance (56)	7-66
Memory and Swap are Consumed at Critical Levels - Maintenance (57)	7-66
Memory and Swap are Consumed at Abnormal Levels - Maintenance (58)	7-67
No Heartbeat Messages Received Through the Interface - Maintenance (61)	7-67
Link Monitor: Interface Lost Communication - Maintenance (62)	7-67
Outgoing Heartbeat Period Exceeded Limit - Maintenance (63)	7-67
Average Outgoing Heartbeat Period Exceeds Major Alarm Limit - Maintenance (64)	7-67
Disk Partition Critically Consumed - Maintenance (65)	7-68
Disk Partition Significantly Consumed - Maintenance (66)	7-68
The Free Inter-Process Communication Pool Buffers Below Minor Threshold - Maintenance (67)	7-68
The Free Inter-Process Communication Pool Buffers Below Major Threshold - Maintenance (68)	7-68

The Free Inter-Process Communication Pool Buffers Below Critical Threshold - Maintenance (69)	7-68
The Free Inter-Process Communication Pool Buffer Count Below Minimum Required - Maintenance (70)	7-69
Local Domain Name System Server Response Too Slow - Maintenance (71)	7-69
External Domain Name System Server Response Too Slow - Maintenance (72)	7-69
External Domain Name System Server not Responsive - Maintenance (73)	7-69
Local Domain Name System Service not Responsive - Maintenance (74)	7-69
Mismatch of Internet Protocol Address Local Server and Domain Name System - Maintenance (75)	7-70
Mate Time Differs Beyond Tolerance - Maintenance (77)	7-70
Bulk Data Management System Admin State Change - Maintenance (78)	7-70
Resource Reset - Maintenance (79)	7-70
Resource Reset Warning - Maintenance (80)	7-70
Resource Reset Failure - Maintenance (81)	7-70
Average Outgoing Heartbeat Period Exceeds Critical Limit - Maintenance (82)	7-71
Swap Space Below Minor Threshold - Maintenance (83)	7-71
Swap Space Below Major Threshold - Maintenance (84)	7-71
Swap Space Below Critical Threshold - Maintenance (85)	7-71
System Health Report Collection Error - Maintenance (86)	7-71
Status Update Process Request Failed - Maintenance (87)	7-71
Status Update Process Database List Retrieval Error - Maintenance (88)	7-72
Status Update Process Database Update Error - Maintenance (89)	7-72
Disk Partition Moderately Consumed - Maintenance (90)	7-72
Internet Protocol Manager Configuration File Error - Maintenance (91)	7-72
Internet Protocol Manager Initialization Error - Maintenance (92)	7-72
Internet Protocol Manager Interface Failure - Maintenance (93)	7-72
Internet Protocol Manager Interface State Change - Maintenance (94)	7-72
Internet Protocol Manager Interface Created - Maintenance (95)	7-73
Internet Protocol Manager Interface Removed - Maintenance (96)	7-73
Inter-Process Communication Input Queue Entered Throttle State - Maintenance (97)	7-73
Inter-Process Communication Input Queue Depth at 25% of its Hi-Watermark - Maintenance (98)	7-73
Inter-Process Communication Input Queue Depth at 50% of its Hi-Watermark - Maintenance (99)	7-73
Inter-Process Communication Input Queue Depth at 75% of its Hi-Watermark - Maintenance (100)	7-74
Switchover in Progress - Maintenance (101)	7-74
Thread Watchdog Counter Close to Expiry for a Thread - Maintenance (102)	7-74
Central Processing Unit is Offline - Maintenance (103)	7-74
Troubleshooting Maintenance Alarms	7-75

Local Side has Become Faulty - Maintenance (3)	7-77
Mate Side has Become Faulty - Maintenance (4)	7-77
Changeover Failure - Maintenance (5)	7-77
Changeover Timeout - Maintenance (6)	7-78
Mate Rejected Changeover - Maintenance (7)	7-78
Mate Changeover Timeout - Maintenance (8)	7-81
Local Initialization Failure - Maintenance (9)	7-81
Local Initialization Timeout - Maintenance (10)	7-81
Process Manager: Process has Died - Maintenance (18)	7-81
Process Manager: Process Exceeded Restart Rate - Maintenance (19)	7-81
Lost Connection to Mate - Maintenance (20)	7-82
Network Interface Down - Maintenance (21)	7-82
Process Manager: Process Failed to Complete Initialization - Maintenance (23)	7-82
Process Manager: Restarting Process - Maintenance (24)	7-82
Process Manager: Going Faulty - Maintenance (26)	7-82
Process Manager: Binary Does not Exist for Process - Maintenance (40)	7-82
Number of Heartbeat Messages Received is Less Than 50% of Expected - Maintenance (42)	7-83
Process Manager: Process Failed to Come Up in Active Mode - Maintenance (43)	7-83
Process Manager: Process Failed to Come Up in Standby Mode - Maintenance (44)	7-83
Application Instance State Change Failure - Maintenance (45)	7-83
Thread Watchdog Counter Expired for a Thread - Maintenance (47)	7-83
Index Table Usage Exceeded Minor Usage Threshold Level - Maintenance (48)	7-84
Index Table Usage Exceeded Major Usage Threshold Level - Maintenance (49)	7-84
Index Table Usage Exceeded Critical Usage Threshold Level - Maintenance (50)	7-84
A Process Exceeds 70% of Central Processing Unit Usage - Maintenance (51)	7-84
The Central Processing Unit Usage is Over 90% Busy - Maintenance (53)	7-84
The Five Minute Load Average is Abnormally High - Maintenance (55)	7-85
Memory and Swap are Consumed at Critical Levels - Maintenance (57)	7-85
No Heartbeat Messages Received Through the Interface - Maintenance (61)	7-85
Link Monitor: Interface Lost Communication - Maintenance (62)	7-85
Outgoing Heartbeat Period Exceeded Limit - Maintenance (63)	7-86
Average Outgoing Heartbeat Period Exceeds Major Alarm Limit - Maintenance (64)	7-86
Disk Partition Critically Consumed - Maintenance (65)	7-86
Disk Partition Significantly Consumed - Maintenance (66)	7-86
The Free Inter-Process Communication Pool Buffers Below Minor Threshold - Maintenance (67)	7-86
The Free Inter-Process Communication Pool Buffers Below Major Threshold - Maintenance (68)	7-87
The Free Inter-Process Communication Pool Buffers Below Critical Threshold - Maintenance (69)	7-87

The Free Inter-Process Communication Pool Buffer Count Below Minimum Required - Maintenance (70)	7-87
Local Domain Name System Server Response Too Slow - Maintenance (71)	7-87
External Domain Name System Server Response Too Slow - Maintenance (72)	7-87
External Domain Name System Server not Responsive - Maintenance (73)	7-88
Local Domain Name System Service not Responsive - Maintenance (74)	7-88
Mate Time Differs Beyond Tolerance - Maintenance (77)	7-88
Average Outgoing Heartbeat Period Exceeds Critical Limit - Maintenance (82)	7-88
Swap Space Below Minor Threshold - Maintenance (83)	7-88
Swap Space Below Major Threshold - Maintenance (84)	7-88
Swap Space Below Critical Threshold - Maintenance (85)	7-89
System Health Report Collection Error - Maintenance (86)	7-89
Status Update Process Request Failed - Maintenance (87)	7-89
Status Update Process Database List Retrieval Error - Maintenance (88)	7-89
Status Update Process Database Update Error - Maintenance (89)	7-89
Disk Partition Moderately Consumed - Maintenance (90)	7-89
Internet Protocol Manager Configuration File Error - Maintenance (91)	7-90
Internet Protocol Manager Initialization Error - Maintenance (92)	7-90
Internet Protocol Manager Interface Failure - Maintenance (93)	7-90
Inter-Process Communication Input Queue Entered Throttle State - Maintenance (97)	7-90
Inter-Process Communication Input Queue Depth at 25% of Its Hi-Watermark - Maintenance (98)	7-90
Inter-Process Communication Input Queue Depth at 50% of Its Hi-Watermark - Maintenance (99)	7-91
Inter-Process Communication Input Queue Depth at 75% of Its Hi-Watermark - Maintenance (100)	7-91
Switchover in Progress - Maintenance (101)	7-91
Thread Watchdog Counter Close to Expiry for a Thread - Maintenance (102)	7-91
Central Processing Unit is Offline - Maintenance (103)	7-91

CHAPTER 8

Operations Support System Troubleshooting 8-1

Introduction	8-1
Operations Support System Events and Alarms	8-2
OSS (1)	8-2
OSS (2)	8-3
OSS (3)	8-3
OSS (4)	8-4
OSS (5)	8-4
OSS (6)	8-5
OSS (7)	8-5

OSS (8) 8-6

OSS (9) 8-6

OSS (10) 8-7

OSS (11) 8-8

Monitoring Operations Support System Events 8-9

Test Report - Operations Support System (1) 8-9

Undefined Variable in Known Set - Operations Support System (2) 8-9

Undefined Data Column Identification - Operations Support System (3) 8-9

Request Handler Instantiation Error - Operations Support System (4) 8-10

Structured Query Language Error While Getting Statistics - Operations Support System (5) 8-10

Structured Query Language Connection Error - Operations Support System (6) 8-10

Simple Network Management Protocol File Read Error - Operations Support System (7) 8-10

No Reply Received from Destination - Operations Support System (8) 8-10

Simple Network Management Protocol Authentication Error - Operations Support System (9) 8-10

Queue Processing Module Database Management Index Failed with Error - Operations Support System (10) 8-11

Queue Processing Module Database Management Index Mismatch During Add or Delete - Operations Support System (11) 8-11

Troubleshooting Operations Support System Alarms 8-12

Undefined Variable in Known Set - Operations Support System (2) 8-12

Undefined Data Column Identification - Operations Support System (3) 8-12

Request Handler Instantiation Error - Operations Support System (4) 8-12

Structured Query Language Error While Getting Statistics - Operations Support System (5) 8-13

Structured Query Language Connection Error - Operations Support System (6) 8-13

No Reply Received from Destination - Operations Support System (8) 8-13

Simple Network Management Protocol Authentication Error - Operations Support System (9) 8-13

Queue Processing Module Database Management Index Failed with Error - Operations Support System (10) 8-14

CHAPTER 9

Security Troubleshooting 9-1

Introduction 9-1

Security Events and Alarms 9-2

SECURITY (1) 9-2

SECURITY (2) 9-2

SECURITY (3) 9-3

SECURITY (4) 9-3

SECURITY (5) 9-4

Monitoring Security Events 9-5

Test Report - Security (1) 9-5

Invalid Credentials Presented by a Session Initiation Protocol Phone - Security (2) 9-5

Internet Protocol Security Connection Down - Security (3)	9-5
Internet Protocol Security Media Terminal Adapter Key Establish Error - Security (4)	9-5
Internet Protocol Security Outgoing Security Association Not Found - Security (5)	9-6
Troubleshooting Security Alarms	9-7
Internet Protocol Security Connection Down - Security (3)	9-7

CHAPTER 10**Signaling Troubleshooting 10-1**

Introduction	10-1
Signaling Events and Alarms	10-2
SIGNALING (1)	10-3
SIGNALING (2)	10-3
SIGNALING (3)	10-4
SIGNALING (4)	10-4
SIGNALING (6)	10-5
SIGNALING (7)	10-5
SIGNALING (8)	10-6
SIGNALING (9)	10-6
SIGNALING (10)	10-7
SIGNALING (11)	10-7
SIGNALING (12)	10-8
SIGNALING (13)	10-8
SIGNALING (14)	10-9
SIGNALING (15)	10-9
SIGNALING (16)	10-10
SIGNALING (17)	10-10
SIGNALING (18)	10-11
SIGNALING (19)	10-11
SIGNALING (20)	10-12
SIGNALING (21)	10-12
SIGNALING (22)	10-13
SIGNALING (23)	10-13
SIGNALING (24)	10-14
SIGNALING (25)	10-14
SIGNALING (26)	10-15
SIGNALING (27)	10-16
SIGNALING (28)	10-17
SIGNALING (29)	10-18
SIGNALING (30)	10-19
SIGNALING (31)	10-20

SIGNALING (32)	10-21
SIGNALING (33)	10-22
SIGNALING (34)	10-23
SIGNALING (36)	10-24
SIGNALING (40)	10-25
SIGNALING (42)	10-25
SIGNALING (43)	10-26
SIGNALING (44)	10-26
SIGNALING (45)	10-27
SIGNALING (46)	10-27
SIGNALING (49)	10-28
SIGNALING (50)	10-28
SIGNALING (51)	10-29
SIGNALING (52)	10-29
SIGNALING (53)	10-30
SIGNALING (54)	10-30
SIGNALING (55)	10-31
SIGNALING (57)	10-31
SIGNALING (58)	10-32
SIGNALING (59)	10-32
SIGNALING (60)	10-33
SIGNALING (61)	10-33
SIGNALING (62)	10-34
SIGNALING (63)	10-34
SIGNALING (64)	10-35
SIGNALING (65)	10-35
SIGNALING (66)	10-36
SIGNALING (68)	10-36
SIGNALING (69)	10-37
SIGNALING (70)	10-37
SIGNALING (71)	10-38
SIGNALING (72)	10-38
SIGNALING (73)	10-39
SIGNALING (74)	10-39
SIGNALING (75)	10-40
SIGNALING (76)	10-40
SIGNALING (77)	10-41
SIGNALING (78)	10-41
SIGNALING (79)	10-42
SIGNALING (80)	10-43

SIGNALING (81)	10-43
SIGNALING (82)	10-44
SIGNALING (83)	10-44
SIGNALING (84)	10-45
SIGNALING (85)	10-45
SIGNALING (86)	10-46
SIGNALING (87)	10-46
SIGNALING (88)	10-47
SIGNALING (89)	10-47
SIGNALING (90)	10-48
SIGNALING (91)	10-48
SIGNALING (92)	10-49
SIGNALING (93)	10-49
SIGNALING (94)	10-50
SIGNALING (95)	10-50
SIGNALING (96)	10-51
SIGNALING (97)	10-51
SIGNALING (98)	10-52
SIGNALING (99)	10-52
SIGNALING (100)	10-53
SIGNALING (101)	10-53
SIGNALING (102)	10-54
SIGNALING (103)	10-54
SIGNALING (104)	10-55
SIGNALING (105)	10-55
SIGNALING (106)	10-56
SIGNALING (107)	10-57
SIGNALING (108)	10-58
SIGNALING (109)	10-58
SIGNALING (110)	10-59
SIGNALING (111)	10-59
SIGNALING (112)	10-60
SIGNALING (113)	10-60
SIGNALING (114)	10-61
SIGNALING (115)	10-61
SIGNALING (116)	10-62
SIGNALING (117)	10-62
SIGNALING (118)	10-63
SIGNALING (119)	10-63
SIGNALING (120)	10-64

SIGNALING (121)	10-64
SIGNALING (122)	10-65
SIGNALING (124)	10-65
SIGNALING (125)	10-66
SIGNALING (126)	10-66
SIGNALING (127)	10-66
SIGNALING (132)	10-67
SIGNALING (133)	10-67
SIGNALING (134)	10-68
SIGNALING (135)	10-68
SIGNALING (136)	10-69
SIGNALING (137)	10-69
SIGNALING (138)	10-70
SIGNALING (139)	10-70
SIGNALING (140)	10-71
SIGNALING (141)	10-71
SIGNALING (142)	10-72
SIGNALING (143)	10-72
SIGNALING (144)	10-73
SIGNALING (145)	10-73
SIGNALING (150)	10-74
Monitoring Signaling Events	10-75
Test Report - Signaling (1)	10-79
Message Encoding Error - Signaling (2)	10-80
Message Decoding Error - Signaling (3)	10-80
Invalid Message Received - Signaling (4)	10-80
Database Module Function Call Failure - Signaling (6)	10-80
Socket Failure - Signaling (7)	10-80
Session Initiation Protocol Message Receive Failure - Signaling (8)	10-81
Timeout on Internet Protocol Address - Signaling (9)	10-81
Failed to Send Complete Session Initiation Protocol Message - Signaling (10)	10-81
Failed to Allocate Session Initiation Protocol Control Block - Signaling (11)	10-81
Feature Server is not Up or is not Responding to Call Agent - Signaling (12)	10-81
Signaling System 7 Signaling Link Down - Signaling (13)	10-81
Link is Remotely Inhibited - Signaling (14)	10-81
Link is Locally Inhibited - Signaling (15)	10-82
Link is Congested - Signaling (16)	10-82
Link: Local Processor Outage - Signaling (17)	10-82
Link: Remote Processor Outage - Signaling (18)	10-82
Link Set Inaccessible - Signaling (19)	10-82

Link Set Congestion - Signaling (20)	10-82
Route Set Failure - Signaling (21)	10-82
Route Set Congested - Signaling (22)	10-83
Destination Point Code Unavailable - Signaling (23)	10-83
Destination Point Code Congested - Signaling (24)	10-83
Unanswered Blocking Message - Signaling (25)	10-83
Unanswered Unblocking Message - Signaling (26)	10-83
Unanswered Circuit Group Blocking Message - Signaling (27)	10-83
Unanswered Circuit Group Unblocking Message - Signaling (28)	10-84
Unanswered Circuit Query Message - Signaling (29)	10-84
Unanswered Circuit Validation Test Message - Signaling (30)	10-84
Unanswered Reset Circuit Message - Signaling (31)	10-84
Unanswered Group Reset Message - Signaling (32)	10-84
Unanswered Release Message - Signaling (33)	10-85
Unanswered Continuity Check Request Message - Signaling (34)	10-85
Trunk Locally Blocked - Signaling (36)	10-85
Trunk Remotely Blocked - Signaling (40)	10-85
Continuity Testing Message Received on the Specified Circuit Identification Code - Signaling (42)	10-85
Release Complete Received in Response to Reset Circuit Message on the Specified Circuit Identification Code - Signaling (43)	10-86
Continuity Recheck is Performed on Specified Circuit Identification Code - Signaling (44)	10-86
Circuit is UNEQUIPPED on Remote Side - Signaling (45)	10-86
Specified Circuit Identification Code is Invalid for the Operation - Signaling (46)	10-86
A General Processing Error Encountered - Signaling (49)	10-86
Unexpected Message for the Call State is Received: Clear Call - Signaling (50)	10-86
Set Trunk State as Remotely Unequipped - Signaling (51)	10-87
Set Trunk State as NOT Remotely Blocked - Signaling (52)	10-87
Set Trunk State as Remotely Blocked - Signaling (53)	10-87
Circuit Validation Test Aborted - Signaling (54)	10-87
Circuit Validation Successful - Signaling (55)	10-87
Continuity Recheck Failed - Signaling (57)	10-87
Continuity Recheck Successful - Signaling (58)	10-87
Auto State Change for Integrated Services Digital Network Trunk Group by Media Gateway - Signaling (59)	10-88
Integrated Services Digital Network STATUS Message Containing Error Indication Received - Signaling (60)	10-88
Trunk Operational State Changed by Service Message - Signaling (61)	10-88
Received Integrated Services Digital Network RESTART Message - Signaling (62)	10-88
Media Gateway/Termination Faulty - Signaling (63)	10-88
Media Gateway Adapter Running out of Shared Memory Pools - Signaling (64)	10-89

Media Gateway Adapter Running out of Heap Memory - Signaling (65)	10-89
Call Agent Internal Error (Because of Which Media Gateway Adapter has to Start Automatically) - Signaling (66)	10-89
Media Gateway or Termination are Found Administratively Out of Service - Signaling (68)	10-89
Call Agent and Feature Server Communication Message Timeout - Signaling (69)	10-89
Integrated Services Digital Network Unable to Restore D-channel Due to Failed Communication - Signaling (70)	10-90
Integrated Services Digital Network Unable to Establish D-channel - Signaling (71)	10-90
Integrated Services Digital Network - Calls Lost Due to D-channel Down for Period of Time - Signaling (72)	10-90
Integrated Services Digital Network - Unable to Send RESTART Due to RESTART Timer Expired - Signaling (73)	10-90
Integrated Services Digital Network: Unable to Send the SERVICE Due to the SERVICE Timer Expired - Signaling (74)	10-91
Signaling System 7 Stack not Ready - Signaling (75)	10-91
Timeout on Remote Instance - Signaling (76)	10-91
Integrated Services Digital Network D-channel Switchover for Non-Facility Associated Signaling - Signaling (77)	10-91
Integrated Services Digital Network Single D-channel Down for Non-Facility Associated Signaling - Signaling (78)	10-91
Media Gateway Unreachable - Signaling (79)	10-92
Out of Bounds, Memory/Socket Error - Signaling (80)	10-92
Insufficient Heap Memory - Signaling (81) (H.323)	10-92
Insufficient Shared Memory Pools - Signaling (82) (H.323)	10-92
Error While Binding to Socket - Signaling (83)	10-92
Reached Maximum Socket Limit - Signaling (84) (H.323)	10-92
Initialization Failure - Signaling (85)	10-92
Remote H323 Gateway is not Reachable - Signaling (86) (H.323)	10-93
H323 Message Parsing Error - Signaling (87) (H.323)	10-93
H323 Message Encoding Error - Signaling (88) (H.323)	10-93
Gatekeeper not Available/Reachable - Signaling (89)	10-93
Alternate Gatekeeper is not Responding - Signaling (90)	10-93
Endpoint Security Violation - Signaling (91) (H.323)	10-93
Invalid Call Identifier - Signaling (92)	10-93
Invalid Call Reference Value - Signaling (93)	10-94
Invalid Conference Identifier - Signaling (94)	10-94
Invalid Message from the Network - Signaling (95)	10-94
Internal Call Processing Error - Signaling (96)	10-94
Insufficient Information to Complete Call - Signaling (97)	10-94
H323 Protocol Inconsistencies - Signaling (98) (H.323)	10-94
Abnormal Call Clearing - Signaling (99)	10-94

Codec Negotiation Failed - Signaling (100)	10-95
Per Call Security Violation - Signaling (101)	10-95
H323 Network Congested - Signaling (102) (H.323)	10-95
Aggregation Connection Down - Signaling (103)	10-95
Aggregation Unable To Establish Connection - Signaling (104)	10-95
Aggregation Gate Set Failed - Signaling (105)	10-95
Enhanced Subscriber Authentication Cisco BTS 10200 Softswitch Delivery Function Connection Down - Signaling (106)	10-96
Logical Internet Protocol Addresses not Mapped Correctly - Signaling (107)	10-96
Current SIA Configuration only Valid for Simplex Systems - Signaling (108)	10-96
Stream Control Transmission Protocol Association Failure - Signaling (109)	10-96
Signaling Gateway Group is Out-of-Service - Signaling (110)	10-96
Stream Control Transmission Protocol Association Degraded (One of Two Internet Protocol Connections Down) - Signaling (111)	10-97
Stream Control Transmission Protocol Association Configuration Error - Signaling (112)	10-97
Signaling Gateway Failure - Signaling (113)	10-97
Signaling Gateway Process is Out-of-Service - Signaling (114)	10-97
Invalid Routing Context Received - Signaling (115)	10-97
Destination Point Code User Part Unavailable - Signaling (116)	10-97
Circuit Validation Test Message Received for an Unequipped Circuit Identification Code - Signaling (117)	10-98
Circuit Verification Response Received with Failed Indication - Signaling (118)	10-98
Signaling System 7 Adapter Process Faulty - Signaling (119)	10-98
Signaling System 7 Module/Signaling System 7 Adapter Faulty - Signaling (120)	10-98
Message Transfer Part 3 User Adapter Cannot Go Standby - Signaling (121)	10-98
Message Transfer Part 3 User Adapter Cannot Go Active - Signaling (122)	10-98
Remote Subsystem is out of Service - Signaling (124)	10-99
Signaling Connection Control Part Routing Error - Signaling (125)	10-99
Signaling Connection Control Binding Failure - Signaling (126)	10-99
Transaction Capabilities Application Part Binding Failure - Signaling (127)	10-99
Transaction Capabilities Application Part Reaches the Provisioned Resource Limit - Signaling (132)	10-99
Unable to Decode Generic Transport Descriptor Message - Signaling (133)	10-99
Signaling System 7 Message Encoding Failure - Signaling (134)	10-100
Signaling System 7 Message Decoding Failure - Signaling (135)	10-100
Signaling System 7 Message Invalid Received - Signaling (136)	10-100
Signaling System 7 Confusion Message Received - Signaling (137)	10-100
Number of Open Session Initiation Protocol Connections is Reaching Engineered Limit - Signaling (138)	10-100
Signaling System 7 Trunk was Found to be in Erroneous State - Signaling (139) (SS7)	10-101
Unanswered Information Message - Signaling (140)	10-101

Address not Resolved by Domain Name System Server - Signaling (141)	10-101
Session Initiation Protocol Trunk Operationally Out-of-Service - Signaling (142)	10-101
Internet Protocol Interface Link to the Signaling System 7 Signaling Gateway is Down - Signaling (143)	10-101
All Internet Interface Links to Signaling System 7 Signaling Gateway are Down - Signaling (144)	10-102
One Internet Protocol Interface to Signaling System 7 Signaling Gateway is Down - Signaling (145)	10-102
Stream Control Transmission Protocol Association Congested - Signaling (150)	10-102
Troubleshooting Signaling Alarms	10-103
Socket Failure - Signaling (7)	10-106
Media Gateway Control Protocol	10-106
Session Initiation Protocol	10-106
Session Initiation Protocol Message Receive Failure - Signaling (8)	10-106
Session Initiation Protocol	10-106
Timeout on Internet Protocol Address - Signaling (9)	10-107
Media Gateway Control Protocol	10-107
Session Initiation Protocol	10-107
Failed to Send Complete Session Initiation Protocol Message - Signaling (10)	10-107
Failed to Allocate Session Initiation Protocol Control Block - Signaling (11)	10-107
Feature Server is not Up or is not Responding to Call Agent - Signaling (12)	10-108
Signaling System 7 Signaling Link Down - Signaling (13)	10-108
Signal System 7 and Call Agent Fail-over Interaction	10-108
Link is Remotely Inhibited - Signaling (14)	10-108
Link is Locally Inhibited - Signaling (15)	10-108
Link is Congested - Signaling (16)	10-109
Link: Local Processor Outage - Signaling (17)	10-109
Link: Remote Processor Outage - Signaling (18)	10-109
Link Set Inaccessible - Signaling (19)	10-109
Link Set Congestion - Signaling (20)	10-109
Route Set Failure - Signaling (21)	10-110
Route Set Congested - Signaling (22)	10-110
Destination Point Code Unavailable - Signaling (23)	10-111
Destination Point Code Congested - Signaling (24)	10-112
Trunk Locally Blocked - Signaling (36)	10-112
Trunk Remotely Blocked - Signaling (40)	10-112
Auto State Change for Integrated Services Digital Network Trunk Group by Media Gateway - Signaling (59)	10-112
Media Gateway/Termination Faulty - Signaling (63)	10-113
Media Gateway Adapter Running out of Shared Memory Pools - Signaling (64)	10-113

Media Gateway Adapter Running out of Heap Memory - Signaling (65)	10-113
Call Agent Internal Error (Because of Which Media Gateway Adapter has to Start Automatically) - Signaling (66)	10-113
Media Gateway or Termination are Found Administratively Out of Service - Signaling (68)	10-114
Call Agent and Feature Server Communication Message Timeout - Signaling (69)	10-114
Signaling System 7 Stack not Ready - Signaling (75)	10-114
Integrated Services Digital Network Single D-channel Down for Non-Facility Associated Signaling - Signaling (78)	10-114
Media Gateway Unreachable - Signaling (79)	10-114
Out of Bounds, Memory/Socket Error - Signaling (80)	10-115
Insufficient Heap Memory - Signaling (81) (H.323)	10-115
Insufficient Shared Memory Pools - Signaling (82) (H.323)	10-115
Error While Binding to Socket - Signaling (83)	10-115
Reached Maximum Socket Limit - Signaling (84) (H.323)	10-115
Initialization Failure - Signaling (85)	10-116
Remote H323 Gateway is not Reachable - Signaling (86) (H.323)	10-116
H323 Message Parsing Error - Signaling (87) (H.323)	10-116
H323 Message Encoding Error - Signaling (88) (H.323)	10-116
Gatekeeper not Available/Reachable - Signaling (89)	10-116
Alternate Gatekeeper is not Responding - Signaling (90)	10-117
Endpoint Security Violation - Signaling (91) (H.323)	10-117
Invalid Call Identifier - Signaling (92)	10-117
Invalid Call Reference Value - Signaling (93)	10-117
Invalid Conference Identifier - Signaling (94)	10-117
Invalid Message from the Network - Signaling (95)	10-118
Internal Call Processing Error - Signaling (96)	10-118
Insufficient Information to Complete Call - Signaling (97)	10-118
H323 Protocol Inconsistencies - Signaling (98) (H.323)	10-118
Abnormal Call Clearing - Signaling (99)	10-118
Codec Negotiation Failed - Signaling (100)	10-119
Per Call Security Violation - Signaling (101)	10-119
H323 Network Congested - Signaling (102) (H.323)	10-119
Aggregation Connection Down - Signaling (103)	10-119
Enhanced Subscriber Authentication Cisco BTS 10200 Softswitch Delivery Function Connection Down - Signaling (106)	10-119
Logical Internet Protocol Addresses not Mapped Correctly - Signaling (107)	10-120
Current SIA Configuration only Valid for Simplex Systems - Signaling (108)	10-120
Stream Control Transmission Protocol Association Failure - Signaling (109)	10-121
Message Transfer Part 3 User Adapter Troubleshooting Procedure	10-121
Signaling Connection Control Part User Adapter Troubleshooting Procedures	10-124

Signaling Gateway Group Is Out-of-Service - Signaling (110)	10-125
Stream Control Transmission Protocol Association Degraded (One of Two Internet Protocol Connections Down) - Signaling (111)	10-125
Message Transfer Part 3 User Adapter Troubleshooting Procedure	10-125
Signaling Connection Control Part User Adapter Troubleshooting Procedure	10-125
Stream Control Transmission Protocol Association Configuration Error - Signaling (112)	10-126
Message Transfer Part 3 User Adapter Troubleshooting Procedure	10-126
Signaling Connection Control Part User Adapter Troubleshooting Procedure	10-126
Signaling Gateway Failure - Signaling (113)	10-126
Signaling Gateway Process Is Out-of-Service - Signaling (114)	10-127
Destination Point Code User Part Unavailable - Signaling (116)	10-127
Circuit Validation Test Message Received for an Unequipped Circuit Identification Code - Signaling (117)	10-127
Circuit Verification Response Received with Failed Indication - Signaling (118)	10-127
Signaling System 7 Adapter Process Faulty - Signaling (119)	10-127
Signaling System 7 Module/Signaling System 7 Adapter Faulty - Signaling (120)	10-128
Message Transfer Part 3 User Adapter Cannot Go Standby - Signaling (121)	10-128
Message Transfer Part 3 User Adapter Cannot Go Active - Signaling (122)	10-128
Remote Subsystem is Out Of Service - Signaling (124)	10-128
Signaling Connection Control Part Routing Error - Signaling (125)	10-129
Signaling Connection Control Part Binding Failure - Signaling (126)	10-129
Transaction Capabilities Application Part Binding Failure - Signaling (127)	10-129
Number of Open Session Initiation Protocol Connections is Reaching Engineered Limit - Signaling (138)	10-129
Session Initiation Protocol Trunk Operationally Out-of-Service - Signaling (142)	10-129
Internet Protocol Interface Link to the Signaling System 7 Signaling Gateway is Down - Signaling (143)	10-130
All Internet Protocol Interface Links to Signaling System 7 Signaling Gateway are Down - Signaling (144)	10-130
One Internet Protocol Interface to Signaling System 7 Signaling Gateway is Down - Signaling (145)	10-130
Stream Control Transmission Protocol Association Congested - Signaling (150)	10-130

CHAPTER 11

Statistics Troubleshooting 11-1

Introduction	11-1
Statistics Events and Alarms	11-2
STATISTICS (1)	11-2
STATISTICS (2)	11-2
STATISTICS (3)	11-3
STATISTICS (4)	11-3
STATISTICS (5)	11-4

STATISTICS (6)	11-4
STATISTICS (7)	11-5
STATISTICS (8)	11-5
STATISTICS (9)	11-6
STATISTICS (10)	11-7
STATISTICS (11)	11-8
STATISTICS (12)	11-9
STATISTICS (13)	11-10
Monitoring Statistics Events	11-11
Test Report - Statistics (1)	11-11
Call Agent Measurement Collection Started - Statistics (2)	11-11
Call Agent Measurement Collection Finished - Statistics (3)	11-11
Plain Old Telephone Service/Centrex/Telecommunications Data Link Monitor Feature Server Measurement Collection Started - Statistics (4)	11-12
Plain Old Telephone Service/Centrex/Telecommunications Data Link Monitor Feature Server Measurement Collection Finished - Statistics (5)	11-12
Advanced Intelligent Network Feature Server Measurement Collection Started - Statistics (6)	11-12
Advanced Intelligent Network Feature Server Measurement Collection Finished - Statistics (7)	11-12
Message Send Failure - Statistics (8)	11-13
Measurement Table Structured Query Language Read Error - Statistics (9)	11-13
Measurement Table Structured Query Language Write Error - Statistics (10)	11-14
Measurement Collection Application Programming Interface Failure - Statistics (11)	11-14
Measurement Handshake Error - Schema Inconsistency - Statistics (12)	11-14
Traffic and Measurements Module Application Programming Interface Failure - Statistics (13)	11-15
Troubleshooting Statistics Alarms	11-16
Measurement Handshake Error - Schema Inconsistency - Statistics (12)	11-16
Traffic and Measurements Module Application Programming Interface Failure - Statistics (13)	11-16

CHAPTER 12

System Troubleshooting 12-1

Introduction	12-1
System Events and Alarms	12-2
SYSTEM (1)	12-2
SYSTEM (2)	12-3
SYSTEM (3)	12-3
SYSTEM (4)	12-4
SYSTEM (5)	12-5
SYSTEM (6)	12-5
SYSTEM (7)	12-6
SYSTEM (8)	12-6

SYSTEM (9)	12-7
SYSTEM (10)	12-7
SYSTEM (11)	12-8
SYSTEM (12)	12-8
Monitoring System Events	12-9
Test Report - System (1)	12-9
Inter-Process Communication Queue Read Failure - System (2)	12-9
Inter-Process Communication Message Allocate Failure - System (3)	12-9
Inter-Process Communication Message Send Failure - System (4)	12-10
Unexpected Inter-Process Communication Message Received - System (5)	12-10
Index List Insert Error - System (6)	12-10
Index List Remove Error - System (7)	12-10
Thread Creation Failure - System (8)	12-10
Timer Start Failure - System (9)	12-10
Index Update Registration Error - System (10)	12-11
Index Table Add-Entry Error - System (11)	12-11
Software Error - System (12)	12-11
Troubleshooting System Alarms	12-12
Inter-Process Communication Queue Read Failure - System (2)	12-12
Inter-Process Communication Message Allocate Failure - System (3)	12-12
Inter-Process Communication Message Send Failure - System (4)	12-12
Index List Insert Error - System (6)	12-13
Index List Remove Error - System (7)	12-13
Thread Creation Failure - System (8)	12-13
Index Update Registration Error - System (10)	12-13
Index Table Add Entry Error - System (11)	12-13
Software Error - System (12)	12-13

CHAPTER 13

Network Troubleshooting 13-1

Introduction	13-1
Troubleshooting a Network Failure	13-1
Verify the Stream Control Transmission Protocol Association Status	13-2
Verify the Configuration	13-3
Verify the Internet Protocol Routing	13-5
Verify if the Application Service Provider is Used by Any Application Server	13-5
Verify the Internet Protocol Transfer Point T1 Card Provisioning	13-5
Verify the Internet Protocol Transfer Point Message Transfer Part 2 Serial Interface	13-6
Verify the Internet Protocol Transfer Point-Signal Transfer Point Linkset Status	13-7
Verify the Internet Protocol Transfer Point Route	13-8

CHAPTER 14**General Troubleshooting 14-1**

Introduction 14-1

Troubleshooting CORBA Problems 14-1

Troubleshooting Local Number Portability Problems 14-2

Resolving Local Number Portability Conflicts 14-2

Audit Requests 14-3

Report Requests 14-3

Troubleshooting Alerting Notification Problems 14-4

Command Responses 14-5

Success and Failure Responses 14-6

Termination Reason Responses 14-8

Trunk Reason Responses 14-10

Trunk Termination Reason Responses, Signaling System 7 Only 14-11

Fault Reason Responses 14-13

Protocol Troubleshooting 14-14

Troubleshooting Signaling System 7 SIGTRAN Problems 14-14

Cisco Internet Protocol Transfer Point Troubleshooting Procedures 14-14

Using Cisco BTS 10200 Softswitch Command Line Interface Commands 14-16

Viewing Cisco BTS 10200 Softswitch Logs 14-17

'Troubleshooting Transaction Capabilities Application Part with the Query Verification Tool 14-17

Debugging Network Related Transaction Capabilities Application Part/Signaling Connection Control Part Problems 14-19

Troubleshooting H.323 Problems 14-25

Outgoing Trunk Group is Out of Service 14-25

Outgoing H.323 Gateway is Out of Service 14-26

H.323 Gateway Fails to Register With Gatekeeper (Invalid Alias) 14-27

Outgoing H.323 Gateway Unregistered With Gatekeeper and Needs to Use Registration, Admissions, and Status 14-28

Stable Calls Are Dropped When Call Agent Switches Over 14-29

No Matching Dial Plan Found on Incoming H.323 Trunk Group 14-29

Configuration at Softswitch or Gatekeeper Has Placed Routing Into a Loop 14-30

Outgoing H.323 Calls Routed to Incorrect Endpoint When Using Registration, Admissions, and Status 14-30

Outgoing H.323 Calls Routed to Incorrect Endpoint When Using Direct Signaling 14-31

Registration, Admissions, and Status Still Used When Outgoing H.323 Call is Provisioned to Use Direct Signaling 14-32

Troubleshooting Integrated Services Digital Network Problems 14-33

How to Troubleshoot When the Integrated Services Digital Network Trunk Group Fails to Restore 14-33

Checking the Status of a Trunk Termination	14-36
Checking Media Gateway Provisioning	14-38
Additional Command Line Interface Verification	14-40
Maintenance of a Call Agent Connected to an Integrated Services Digital Network Trunk Group	14-41
File Configuration – bts.properties	14-42
Editing – bts.properties	14-42
Example Edit – bts.properties	14-43

CHAPTER 15

Diagnostic Tests 15-1

Introduction	15-1
Media Gateway Tests	15-2
Subscriber Termination Tests	15-4
Signaling System 7 Trunk Termination Tests	15-6
Integrated Services Digital Network Trunk Termination Tests	15-10
Channel-Associated Signaling Trunk Termination Tests	15-11
Announcement Trunk Termination Tests	15-13
Troubleshooting Using Snoop	15-15
Query Verification Tool and Translation Verification Tool	15-19
Tool Requirements	15-19
Query Verification Tool	15-19
Overview	15-19
Command Format	15-20
Response Format	15-21
Query Errors	15-22
Query Verification Tool Measurements	15-26
Translation Verification Tool	15-26
Overview	15-26
Command Format	15-26
Response Format	15-27
Translation Verification Tool Measurements	15-28
Using Query Verification Tool and Translation Verification Tool Together	15-28
Network Loopback Test for Network-based Call Signaling/Media Gateway Control Protocol Endpoints	15-30
Overview	15-30
Restrictions	15-31
Installing	15-31
Configuring	15-31
Configuration Examples	15-32

Using/Operating the Network Loopback Test for Network-based Call Signaling/Media Gateway Control Protocol Endpoints	15-32
Dedicated Test Trunk Group	15-33
Shared Test Trunk Group	15-33
Configuring the Originating Trunk Group	15-34
Session Initiation Protocol Subscriber Registration Status Check	15-35
System Health Report	15-36

CHAPTER 16

Disaster Recovery Procedures 16-1

CHAPTER 17

Disk Replacement 17-1

APPENDIX A

System Usage of MGW Keepalive Parameters, Release 4.4.x A-1

Provisionable Parameters	A-2
Definitions and Additional Parameters	A-3
Examples of Successful MGCP Message Transmissions	A-3
Initial AUEP Transmission Successful	A-4
Scenarios with Retransmissions	A-4
Keepalive Process	A-8
Scenario 1—MGW Reachable	A-8
Basic Scenario	A-9
MGCP Message Sent and Is Unsuccessful	A-10
MGCP Message Sent and Is Successful	A-11
Scenario 2 (Special Case)—Reachable RGW with 16 or Fewer Endpoints and No Stable Calls In Progress	A-11
Basic Scenario	A-12
MGCP Message Sent and Is Unsuccessful	A-13
MGCP Message Sent and Is Successful	A-14
Scenario 3—MGW Unreachable	A-15
Release 4.4.0—KA Attempts Unsuccessful, MGW Unreachable	A-15
Releases 4.4.1 and Later—KA Attempts Unsuccessful, MGW Unreachable	A-16
Releases 4.4.1 and Later—MGW Unreachable, New Call Termination Attempt Occurs	A-18



Preface

Revised: October 23, 2008, OL-11335-06

Introduction

This document provides detailed troubleshooting procedures for the Cisco BTS 10200 Softswitch. It provides the procedures for troubleshooting network, subscriber, billing, operations and maintenance, system administrative problems. It also includes details for aiding troubleshooting by utilizing diagnostic and trace procedures.

Objective

The maintenance personnel/troubleshooter of a Cisco BTS 10200 Softswitch can use this document to better understand how to troubleshoot the Cisco BTS 10200 Softswitch and quickly clear network problems.

Audience

This document is designed for engineers, technicians, and system administrators who troubleshoot and repair the Cisco BTS 10200 Softswitch.

Organization

This Troubleshooting Guide contains the following chapters:

- [Chapter 1, “Troubleshooting Overview”](#) – Provides an overview of troubleshooting the Cisco BTS 10200 Softswitch.
- [Chapter 2, “Audit Troubleshooting”](#) – Provides the information needed to monitor and troubleshoot Audit events and alarms.
- [Chapter 3, “Billing Troubleshooting”](#) – Provides the information needed to monitor and troubleshoot Billing events and alarms.
- [Chapter 4, “Call Processing Troubleshooting”](#) – Provides the information needed to monitor and troubleshoot Call Processing events and alarms.
- [Chapter 5, “Configuration Troubleshooting”](#) – Provides the information needed to monitor and troubleshoot Configuration events and alarms.
- [Chapter 6, “Database Troubleshooting”](#) – Provides the information needed to monitor and troubleshoot Database events and alarms.
- [Chapter 7, “Maintenance Troubleshooting”](#) – Provides the information needed to monitor and troubleshoot Maintenance events and alarms.
- [Chapter 8, “Operations Support System Troubleshooting”](#) – Provides the information needed to monitor and troubleshoot Operations Support System events and alarms.
- [Chapter 9, “Security Troubleshooting”](#) – Provides the information needed to monitor and troubleshoot Security events and alarms.
- [Chapter 10, “Signaling Troubleshooting”](#) – Provides the information needed to monitor and troubleshoot Signaling events and alarms.
- [Chapter 11, “Statistics Troubleshooting”](#) – Provides the information needed to monitor and troubleshoot Statistics events and alarms.
- [Chapter 12, “System Troubleshooting”](#) – Provides the information needed to monitor and troubleshoot System events and alarms.
- [Chapter 13, “Network Troubleshooting”](#) – Provides the information needed to conduct network troubleshooting on the Cisco BTS 10200 Softswitch.
- [Chapter 14, “General Troubleshooting”](#) – Provides the general troubleshooting information needed to conduct troubleshooting on the Cisco BTS 10200 Softswitch.
- [Chapter 15, “Diagnostic Tests”](#) – Describes the diagnostic tests that can be performed on media gateways, subscriber terminations, and trunk terminations.
- [Chapter 16, “Disaster Recovery Procedures”](#) – Describes how to recover the database in a disaster situation, how to recover the database from another database, and how to recover data from the Call Agent shared memory.
- [Chapter 17, “Disk Replacement”](#) – Describes how to manually recover a Cisco BTS 10200 Softswitch system.
- [Appendix A, “System Usage of MGW Keepalive Parameters, Release 4.4.x”](#) – Explains how the Cisco BTS 10200 Softswitch determines the connectivity status between itself and a media gateway (MGW)

Conventions

This document uses the following conventions:



Note

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



Caution

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

Updates to this Document for Release 4.4

This document is new for Release 4.4.

Added the following information for version OL-11335-02 of the document:

- [Appendix A, “System Usage of MGW Keepalive Parameters, Release 4.4.x”](#)

Updated the following information for version OL-11335-03 of the document:

- [Appendix A, “System Usage of MGW Keepalive Parameters, Release 4.4.x”](#)

For version OL-11335-05 of the document the Threshold/Throttle information in [Chapter 1, “Troubleshooting Overview”](#) was updated.

For version OL-1133506 of the document Audit 4 alarm information was updated.

Obtaining Documentation

Cisco provides several ways to obtain documentation, technical assistance, and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

Cisco.com

You can access the most current Cisco documentation on the World Wide Web at this universal resource locator (URL):

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

You can access the Cisco website at this URL:

<http://www.cisco.com>

International Cisco websites can be accessed from this URL:

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

Documentation CD-ROM

Cisco documentation and additional literature are available in a Cisco Documentation compact disk - read only media (CD-ROM) package, which may have shipped with your product. The Documentation CD-ROM is updated regularly and may be more current than printed documentation. The CD-ROM package is available as a single unit or through an annual or quarterly subscription.

Registered Cisco.com users can order a single Documentation CD-ROM (product number DOC-CONDOCCD=) through the Cisco Ordering tool:

http://www.cisco.com/en/US/partner/ordering/ordering_place_order_ordering_tool_launch.html

All users can order annual or quarterly subscriptions through the online Subscription Store:

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

Ordering Documentation

You can find instructions for ordering documentation at this URL:

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

You can order Cisco documentation in these ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Networking Products MarketPlace:

<http://www.cisco.com/en/US/partner/ordering/index.shtml>

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

Documentation Feedback

You can submit comments electronically on Cisco.com. On the Cisco Documentation home page, click **Feedback** at the top of the page.

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

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

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

We appreciate your comments.

Obtaining Technical Assistance

For all customers, partners, resellers, and distributors who hold valid Cisco service contracts, the Cisco Technical Assistance Center (TAC) provides 24-hour, award-winning technical support services, online and over the phone. Cisco.com features the Cisco TAC website as an online starting point for technical assistance.

Cisco TAC Website

The Cisco TAC website (<http://www.cisco.com/tac>) provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The Cisco TAC website is available 24 hours a day, 365 days a year.

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

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

Opening a TAC Case

The online TAC Case Open Tool (<http://www.cisco.com/tac/caseopen>) is the fastest way to open S3 and S4 cases. (Your network is minimally impaired or you require product information). After you describe your situation, the TAC Case Open Tool automatically recommends resources for an immediate solution. If your issue is not resolved using these recommendations, your case will be assigned to a Cisco TAC engineer.

For S1 or S2 cases (your production network is down or severely degraded) or if you do not have Internet access, contact Cisco TAC by telephone. Cisco TAC engineers are assigned immediately to S1 and S2 cases to help keep your business operations running smoothly.

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

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

EMEA: +32 2 704 55 55

USA: 1 800 553-2447

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

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

TAC Case Priority Definitions

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

Severity 1 (S1)—Your network is “down” or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Severity 2 (S2)—Operation of an existing network is severely degraded, or significant aspects of your business operation are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Severity 3 (S3)—Operational performance of your network is impaired, but most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Severity 4 (S4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

Obtaining Additional Publications and Information

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

- *The Cisco Product Catalog* describes the networking products offered by Cisco Systems, as well as ordering and customer support services. Access the *Cisco Product Catalog* at this URL:

http://www.cisco.com/en/US/products/products_catalog_links_launch.html

- Cisco Press publishes a wide range of networking publications. Cisco suggests these titles for new and experienced users: Internetworking Terms and Acronyms Dictionary, Internetworking Technology Handbook, Internetworking Troubleshooting Guide, and the Internetworking Design Guide. For current Cisco Press titles and other information, go to Cisco Press online at this URL:

<http://www.ciscopress.com>

- Packet magazine is the Cisco quarterly publication that provides the latest networking trends, technology breakthroughs, and Cisco products and solutions to help industry professionals get the most from their networking investment. Included are networking deployment and troubleshooting tips, configuration examples, customer case studies, tutorials and training, certification information, and links to numerous in-depth online resources. You can access Packet magazine at this URL:

<http://www.cisco.com/go/packet>

- iQ Magazine is the Cisco bimonthly publication that delivers the latest information about Internet business strategies for executives. You can access iQ Magazine at this URL:

<http://www.cisco.com/go/iqmagazine>

- Internet Protocol Journal is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:

http://www.cisco.com/en/US/about/ac123/ac147/about_cisco_the_internet_protocol_journal.html

- Training—Cisco offers world-class networking training. Current offerings in network training are listed at this URL:

<http://www.cisco.com/en/US/learning/index.html>



CHAPTER 1

Troubleshooting Overview

Revised: October 23, 2008, OL-11335-06

Introduction

The telephony industry is rapidly moving toward increasingly complex environments, involving multiple media types, multiple protocols, and interconnections to a wide variety of networks. These new networks may be transit networks belonging to an Internet service provider (ISP) or telcos that interconnect with private networks. The convergence of voice, data, and video into these types of networks has also added to the complexity and the importance of network reliability.

More complex network environments mean that the potential for connectivity and performance problems in internetworks is high, and the source of problems is often elusive. This guide describes methodologies, techniques, and procedures for troubleshooting problems that might arise in the day-to-day operations of a telephony solution that employs the Cisco BTS 10200 Softswitch.

Interoperability

The Cisco BTS 10200 Softswitch inter-works with a wide range of NEs, but there are certain limitations. Cisco recommends that you keep the following caution in mind as you prepare to purchase and use NEs for your network.



Caution

Some features involve the use of other NEs deployed in the service provider network, for example, gateways, media servers, announcement servers, MTAs, and Session Initiation Protocol (SIP) phones. See the “Component Interoperability” section of the Release Notes document for a complete list of the specific peripheral platforms, functions, and software loads that have been used in system testing for interoperability with the Cisco BTS 10200 Softswitch Release 4.5 software. Earlier or later releases of platform software might be interoperable and it might be possible to use other functions on these platforms. The list certifies only that the required inter-operation of these platforms, the functions listed, and the protocols listed have been successfully tested with the Cisco BTS 10200 Softswitch.

Symptoms, Problems, and Solutions

Failures in networks are often characterized by certain symptoms. These symptoms might be general (such as clients being incapable of accessing specific numbers) or more specific (routes not existing in a routing table). In most cases symptoms can be traced to one or more problems or causes by using specific troubleshooting tools and techniques. After being identified, problems can usually be remedied by implementing a solution consisting of a series of specific actions.

This guide describes how to define symptoms, identify problems, and implement solutions in those environments employing a Cisco BTS 10200 Softswitch. You should always apply the specific context in which you are troubleshooting to determine how to detect symptoms and diagnose problems for your specific environment.

If you are having difficulty installing or starting your Cisco BTS 10200 Softswitch, it could be caused by provisioning problems, or by problems with initial status or control settings. If this is the case, your system should display one or more status or error messages. These messages are described in detail in the following chapters along with the probable cause and recommended action(s). General information about the managing the alarm and error messages is provided in [Managing Events and Alarms, page 1-8](#).

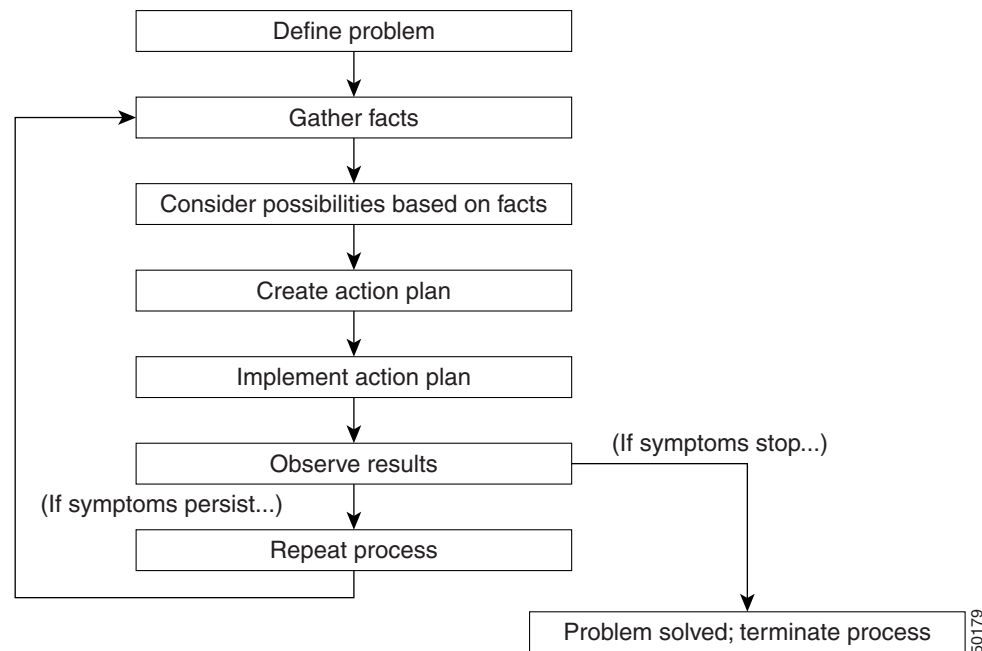
General Problem-Solving Model

When you're troubleshooting in a telephony environment, a systematic approach always works best. An unsystematic approach to troubleshooting can result in a "quick fix," but it is usually a waste of valuable time and resources and often makes the situation worse.

A systematic approach employs the following steps:

- Define the specific symptoms
- Identify all potential problems that could be causing the symptoms
- Systematically eliminate each potential problem (from the most likely to the least likely) until the symptoms disappear

[Figure 1-1](#) illustrates the process flow for the general problem-solving model. This process flow is not a rigid outline for troubleshooting a network; it is simply a foundation from which you can build a problem-solving process to suit your particular environment.

Figure 1-1 General Problem-Solving Model

The following steps detail the problem-solving process outlined in [Figure 1-1](#):

-
- Step 1** When analyzing a network problem, make a clear problem statement. You should define the problem in terms of a set of symptoms and potential causes.
- To properly analyze the problem, identify the general symptoms and then ascertain what kinds of problems (causes) could result in these symptoms. For example, hosts might not be responding to service requests from clients (a symptom). Possible causes might include a mis-configured host, bad interface cards, or missing router configuration commands.
- Step 2** Gather the facts that you need to help isolate possible causes.
- Ask questions of affected users, network administrators, system managers, and other key people. Collect information from sources such as network management systems, protocol analyzer traces, output from diagnostic commands, or the software release notes.
- Step 3** Consider possible problems based on the facts that you gathered. Using the facts, you can eliminate some of the potential problems from your list.
- Depending on the data, for example, you might be able to eliminate hardware as a problem so that you can focus on software problems. At every opportunity, try to narrow the number of potential problems so that you can create an efficient plan of action.
- Step 4** Create an action plan based on the remaining potential problems. Begin with the most likely problem, and devise a plan in which only one variable is manipulated.
- Changing only one variable at a time enables you to reproduce a given solution to a specific problem. If you alter more than one variable simultaneously, you might solve the problem, but identifying the specific change that eliminated the symptom becomes far more difficult and will not help you solve the same problem if it occurs in the future.
- If a variable change does not resolve the network problem, change the variable back to its initial setting before proceeding. This allow the resolution of the network problem to be traced to a single variable change instead of a combination of variable changes.

- Step 5** Implement the action plan, performing each step carefully while testing to see whether the symptom disappears.
- Whenever you change a variable, be sure to gather results. Generally, you should use the same method of gathering facts that you used in Step 2 (that is, working with the key people affected, in conjunction with utilizing your diagnostic tools).
- Step 6** Analyze the results to determine whether the problem has been resolved. If it has, then the process is complete.
- Step 7** If the problem has not been resolved, you must create an action plan based on the next most likely problem in your list. Return to Step 4, change one variable at a time, and repeat the process until the problem is solved.

**Note**

If you exhaust all the common causes and actions—either those outlined in this book or ones that you have identified for your environment—you should contact your Cisco technical support representative.

Resolving Network Problems

It is always easier to recover from a network failure if you are prepared for it ahead of time. Possibly the most important requirement in any network environment is to have current and accurate information about that network available to the network support personnel. Intelligent decisions can be made about network change only with complete information, and troubleshooting be done as quickly and as easily as possible. Downtime in a telephony environment means loss of service to customers, which means an interruption in the revenue stream that supports that network.

During the process of network troubleshooting, the network is expected to exhibit abnormal behavior. Therefore, it is always a good practice to set up a maintenance time window for troubleshooting to minimize any business impact. Always document any changes being made so that it is easier to back out if your troubleshooting approach has failed to identify the problem within the maintenance window.

To determine whether you are prepared for a network failure, answer the following questions:

- Do you have an accurate physical and logical map of your network?
Does your organization or department have an up-to-date network map that outlines the physical location of all the devices on the network and how they are connected, as well as a logical map of network addresses, network numbers, subnetworks, and so forth?
- Do you have a list of all network protocols implemented in your network?
For each of the protocols implemented, do you have a list of the network numbers, subnetworks, zones, areas, and so on that are associated with them?
- Do you know which protocols are being used to route calls?
For each protocol, do you have correct, up-to-date configuration information?
- Do you know all the points of contact to external networks, including any connections to the Internet, the public switched telephone network (PSTN), or the Signaling System 7 (SS7) network?
For each external network connection, do you know what protocol(s) are being used?
- Do you have an established baseline for your network?
Has your organization documented normal network behavior and performance at different times of the day so that you can compare the current problems with a baseline?

If you can answer yes to all of these questions, you will be able to recover from a failure more quickly and more easily than if you are not prepared. Lastly, for every problem solved, be sure to document the problems with solutions provided. This way, you will create a problem/answer database that others in your organization can refer to in case similar problems occur later. This will invariably reduce the time to troubleshoot your networks and, consequently, minimize your business impact.

Resolving System Problems

If the procedures presented in this guide do not clear the problems, contact your technical support group. If additional support is needed, contact Cisco Technical Assistance Center (TAC) for assistance.

When possible, have the following information on hand before calling Cisco TAC for technical support:

- Alarms currently active on the system
- Summary of events that may be related to this problem
- Current status of internal and external components (administrative and operational states)
- Hardware documentation and cabling diagrams, if applicable

Follow the procedure shown in [Figure 1-2](#) to identify a potential problem. If restoral of database, application, or operating system (OS) is required, or if hardware repair is required, use the procedures shown in [Figure 1-3](#). The restoral procedures shown in [Figure 1-3](#) are used only on Cisco BTS 10200 Softswitch systems that are *not* carrying live traffic.



Caution

These are not upgrade procedures. Performing the steps in these restoral procedures brings the platform down and stops call processing. Do not run them on an active system that is carrying live traffic. If you have questions, contact Cisco TAC.



Caution

If both the active and standby database become corrupted, contact Cisco TAC immediately. Refer to the [“Obtaining Technical Assistance” section on page xxxviii](#) for detailed instructions on contacting Cisco TAC and opening a service request.



Caution

If both an active and standby application file becomes corrupted, contact Cisco TAC immediately. Refer to the [“Obtaining Technical Assistance” section on page xxxviii](#) for detailed instructions on contacting Cisco TAC and opening a service request.

Figure 1-2 **Problem Identification**

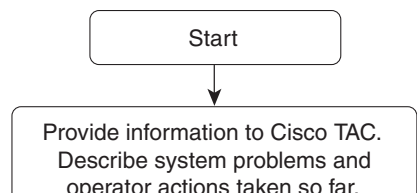
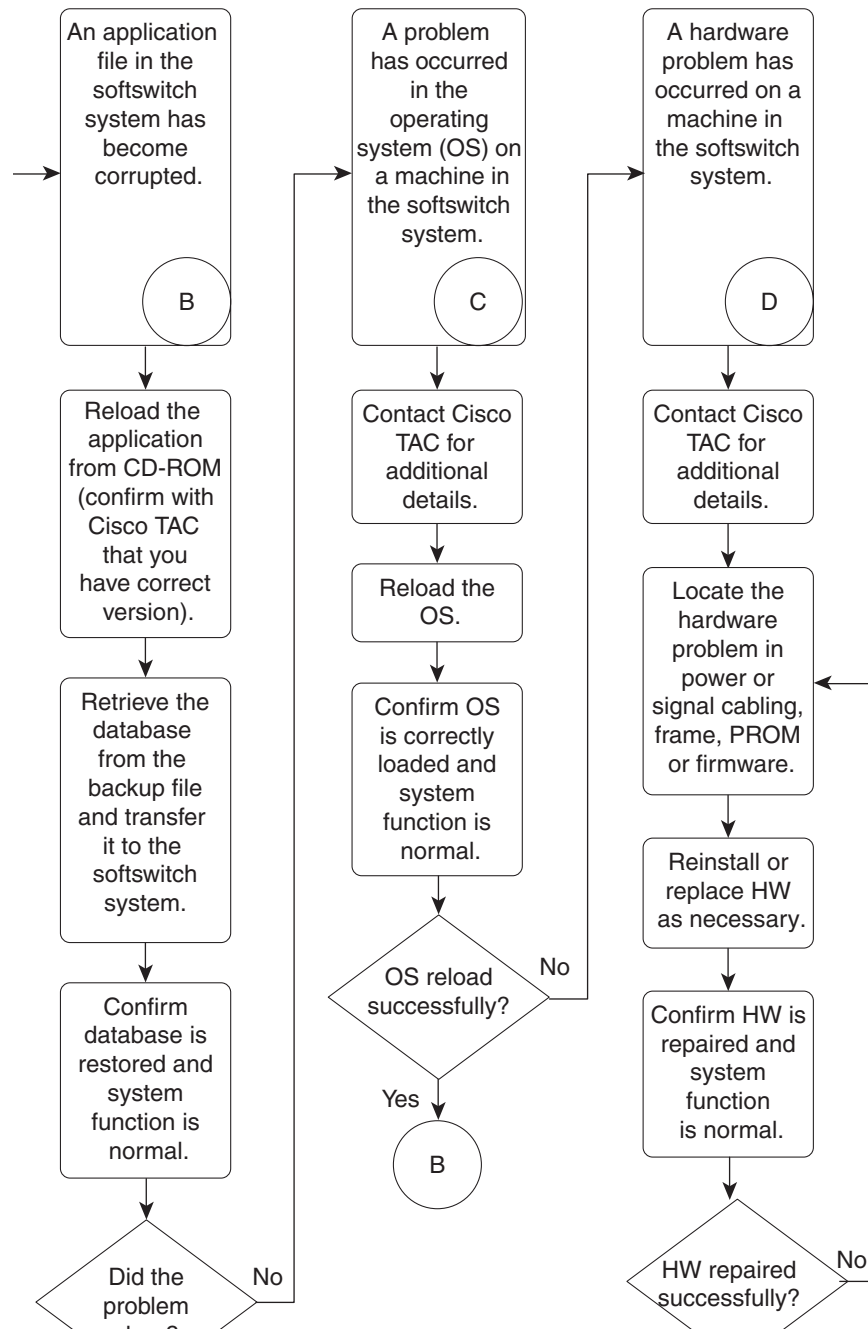


Figure 1-3 **Resolving Database, Application, OS and Hardware Problems**



Managing Events and Alarms

The Cisco BTS 10200 Softswitch generates messages or events to notify you of network conditions. Events with severity levels of critical, major, and minor are classified as alarms. Events and alarms are reported to the operator console and can be retrieved through command line interface (CLI) commands or a Simple Network Management Protocol (SNMP) manager.

The Cisco BTS 10200 Softswitch software writes event and alarm messages to log files that are set up during system initialization. This chapter provides information on using and working with event and alarm log files.

Alarms and informational events produce different system responses.

- An alarm is reported whenever an alarmed state changes.
- An informational event is reported just once, upon its occurrence, through the operator interfaces without any state change being required.

An informational event indicates that a condition worthy of note has occurred. An invalid protocol call state transition is an example of an informational event.

This section contains the following:

- [Managing Event and Alarm Reports, page 1-9](#)
 - [Show Alarm Command, page 1-9](#)
 - [Report Alarm Command, page 1-10](#)
 - [Ack Alarm Command, page 1-11](#)
 - [Clear Alarm Command, page 1-11](#)
 - [Format of Alarm Reports, page 1-12](#)
- [Events and Alarm Logs, page 1-13](#)
- [Viewing Event or Alarm Logs, page 1-13](#)
 - [Show, Add, and Delete Event Queue Commands, page 1-15](#)
- [Saving Events to Log Files, page 1-15](#)
 - [Show Report-Properties Command, page 1-15](#)
 - [Changing Report Properties, page 1-15](#)
 - [Changing Threshold and Throttle Values, page 1-16](#)
 - [Managing and Responding to Events and Alarms, page 1-17](#)
- [Events and Alarms Descriptions and Corrective Actions, page 1-18](#)
 - [Format of Events and Alarms, page 1-18](#)

**Note**

Refer to the *Cisco BTS 10200 Softswitch Command Line Interface Reference Guide*, Release 4.5 for a detailed description of all commands and tokens discussed in this chapter.

Managing Event and Alarm Reports

There are two ways to view events and alarms—by subscribing to event and alarm reports (automatic, real-time) and by retrieving event or alarm summaries from the log files by operator query.

Use the following **subscribe** commands to subscribe to reports of real-time events or alarms:

```
subscribe event-report type=<type>; severity=<severity>;
subscribe alarm-report type=<type>; severity=<severity>;
```



Note

In the **subscribe event-report** or **subscribe alarm-report** commands you can specify “type=all” and/or “severity=all” or you can specify the specific types and severities of events and alarms you wish to display. Specifying all allows you to monitor the system for *all* events or alarms. Specifying a specific type and a specific severity allows you to monitor the system for the specified type and severity of events and alarms. The default type and severity is “all”.

Show Alarm Command

Use the **show alarm** command to view all real-time alarms. All of the following tokens are optional.

```
show alarm id=<sn>; type=<type>; number=<num>; severity=<sev>;
component-id=<comp>; origin=<process>; start-time=<yyyy-mm-dd hh:mm:ss>;
end-time=<yyyy-mm-dd hh:mm:ss>
```



Note

If the **show alarm** command is issued without any tokens (parameters), *all* alarms of *all* types for *all* components are displayed. Issuing the **show alarm** command with *any* combination of the optional tokens limits the display to a subset of alarms as determined by which optional tokens are specified.

The **show alarm** command can include any or all the following optional tokens:

- **id**—The unique system-assigned serial number of an alarm.
- **type**—Type of alarm to show, which can be any one of the following:
 - audit
 - billing
 - callp
 - config
 - database
 - maintenance
 - oss
 - security
 - signaling
 - statistics
 - system
- **number**—The numerical identifier of the alarm of the specified type (1 to 500).

Specifying a type and a number shows only alarms of that type and number. You can specify a number without specifying a type; and you can specify a type without specifying a number.

- **severity**—The severity level of the alarm, which can be any one of the following:
 - critical
 - major
 - minor
- **origin**—The internal designation of the process generating the alarm(s) (1 to 64 ASCII characters).
- **component-id**—The identification (ID) of the component reporting the alarm(s) (1 to 32 ASCII characters).
- **start-time** or **end-time**—Timestamp indicating the time the monitoring of the specified alarm states should start or end in the format yyyy-mm-dd hh:mm:ss where:
 - yyyy—year (4-digit number)
 - mm—month (01 to 12)
 - dd—day (01 to 31)
 - hh—hour (00 to 23)
 - mm—minute (00 to 59)
 - ss—second (00 to 59)

Report Alarm Command

Use the **report alarm** command to view all real-time alarms. All of the following tokens are optional.

```
report alarm id=<sn>; type=<type>; number=<num>; severity=<sev>;
component-id=<comp>; origin=<process>; output=<file name>; output-type=<file
type>; <start-time=yyyy-mm-dd hh:mm:ss>; end-time=<yyyy-mm-dd hh:mm:ss>
```



Note

If the **report alarm** command is issued without any tokens (parameters), *all* alarms of *all* types for *all* components are displayed. Issuing the **report alarm** command with *any* combination of the optional tokens limits the display to a subset of alarms as determined by which optional tokens are specified.

The **report alarm** command can include any or all the following optional tokens:

- **id**—The unique system-assigned serial number of an alarm.
- **type**—Type of alarm to show, which can be any one of the following:
 - audit
 - billing
 - callp
 - config
 - database
 - maintenance
 - oss
 - security
 - signaling
 - statistics
 - system

- **number**—The numerical identifier of the alarm of the specified type (1 to 500).
Specifying a type and a number shows only alarms of that type and number. You can specify a number without specifying a type; and you can specify a type without specifying a number.
- **severity**—The severity level of the alarm, which can be any one of the following:
 - critical
 - major
 - minor
- **origin**—The internal designation of the process generating the alarm(s) (1 to 64 ASCII characters).
- **output**—The name of the output file.
- **output-type**—The type of output file.
- **component-id**—The identification (ID) of the component reporting the alarm(s) (1 to 32 ASCII characters).
- **start-time** or **end-time**—Timestamp indicating the time the monitoring of the specified alarm states should start or end in the format yyyy-mm-dd hh:mm:ss where:
 - yyyy—year (4-digit number)
 - mm—month (01 to 12)
 - dd—day (01 to 31)
 - hh—hour (00 to 23)
 - mm—minute (00 to 59)
 - ss—second (00 to 59)

Ack Alarm Command

Use the **ack alarm** command to acknowledge an alarm, i.e. to turn off the alarm bell.

```
ack alarm id=<sn>;
```

The ID token is required for the ack alarm command, which acknowledges only the specified alarm.



Note

The Ack Alarm command only applies to Cisco BTS 10200 Softswitch systems with the optional Call Control Unit (CCU) Alarm Panel installed.

Clear Alarm Command

Use the **clear alarm** command to clear an alarm.

```
clear alarm id=<sn>;
```

The ID token is required for the **clear alarm** command, when only the specified alarm is to be cleared.

To clear all alarms, use the following command.

```
clear alarm forced=Y
```



Note

When an alarm is cleared a new alarm event will be generated if the alarm condition still exists.

Format of Alarm Reports

The general format of an alarm report, as displayed on an operator console, is shown below. An alarm summary contains multiple alarm reports, selected according to the query that is entered. For example, the following query produced the result shown here.

```
show alarm type=callp; number=23; component-id=tml@cal.carrier.com
```

```
Reply: Success: Request was successfully completed
ID=123456
TYPE=callp
NUMBER=23
TEXT=Trunk Group Out Of Service
STATUS=ACKNOWLEDGED
SEVERITY=MAJOR
TIME=2004-04-23 10:54:20
COMPONENT ID=tml@cal.carrier.com
ORIGIN=bcm@cal146
THREAD=
DATAWORD1=
  through
DATAWORD8=
```

Table 1-1 describes the format of event and alarm reports.

Table 1-1 **Format of Event and Alarm Reports**

Event or Alarm Report Contents	Description
Event or Alarm Number	All events and alarms have a unique, system-assigned ID token number.
Event or Alarm Type	Type is the designated category of the report: AUDIT, BILLING, call processing (CALLP), CONFIG, DATABASE, MAINTENANCE, operations support system (OSS), SECURITY, SIGNALING, STATISTICS, or SYSTEM.
Event or Alarm Number	Event or alarm numbers are preset in the Cisco BTS 10200 Softswitch. They are not provisionable and cannot be changed.
Event or Alarm Description	Up to an 80-character description of the event or alarm.
Alarm Status	Status for an alarm can be ALARM_ON, ALARM_OFF, or ALARM_IGNORE.
Event or Alarm Severity	Event Severity: Information (INFO), WARNING, MINOR, MAJOR, or CRITICAL Alarm Severity: MINOR, MAJOR, or CRITICAL
Event or Alarm Date and Time	Date and time of report in the format yyyy-mm-dd hh:mm:ss. Year, month, and day plus hours, minutes, and seconds of an alarm or event, displayed in Greenwich Mean Time (GMT).
Event or Alarm Component ID	ID for the component reporting the event or alarm, for example, tml@cal.carrier.com.
Event or Alarm Origin	ID for the process generating the event or alarm.
Event or Alarm Thread	Thread within the Cisco BTS 10200 Softswitch process that initially issued the alarm.
Event or Alarm Datawords=	Header for additional data fields to an event or alarm. Up to 8 data fields can be reported, depending on the event or alarm. These are the cause and actions listed for each event/alarm.

Events and Alarm Logs

It is recommended that you manage the event and alarm logs in a manner that permits the operator to access all events and alarms and watch for unexpected events or alarms. For example, if any of the following anomalies are seen, investigate promptly to determine the required action:

- Congestion warnings
- Routing errors
- Termination failures
- Billing errors
- Security warnings
- Diagnostic failures
- Process failovers

Viewing Event or Alarm Logs

Use the following **show** commands to view event or alarm logs. The event and alarm logs are typically used if the user session is disrupted, or if all events or alarms of one kind are needed in a single report.

```
show event-log id=<sn>; type=<type>; number=<num>; severity=<severity>;  
component-id= <component-id>; origin=<process-id>;  
start-time=<yyyy-mm-dd hh:mm:ss>; end-time=<yyyy-mm-dd hh:mm:ss>;  
show alarm-log id=<sn>; type=<type>; number=<num>; severity=<severity>;  
component-id=<component-id>; origin=<process-id>;  
start-time=<yyyy-mm-dd hh:mm:ss>; end-time=<yyyy-mm-dd hh:mm:ss>;
```

**Note**

If the **show event-log** or **show alarm-log** commands are issued without any tokens (parameters), *all* events or alarms of *all* types and *all* severities for *all* components are displayed.

Issuing the **show event-log** or **show alarm-log** commands with any combination of optional tokens limits the display to a subset of events or alarms as determined by the optional tokens specified.

By default the 30,000 entries are maintained in the Event/Alarm logs (currently in MySQL database). For every 30 minute interval the event generator (EGA) retains the most recent 30,000 entries in the log. All entries above this are deleted, i.e. if you do a **show alarm-log limit=1**; and reply says 1 of 32008, then EGA would delete the 8 oldest entries.

**Note**

If the **show event-log** or **show alarm-log** commands are issued without any tokens (parameters), up to 30,000 entries may be scrolled across the screen with no way to stop it. It may take an extended period of time to display all entries. These commands should ordinarily be issued with optional tokens.

The **show** commands can include any or all of the following optional tokens:

- **id**—The unique serial number of the event or alarm assigned by the system.
- **type**—The type of event or alarm to show, which can be any one of the following:
 - audit
 - billing
 - callp
 - config
 - database
 - maintenance
 - oss
 - security
 - signaling
 - statistics
 - system
- **number**—The numerical identifier of the event or alarm of the specified type (1 to 500).
- **severity**—The severity level of the event or alarm, which can be any one of the following:
 - critical
 - major
 - minor
 - warning (events only)
 - info (events only)
- **origin**—The internal designation of the process generating the event or alarm (1 to 64 ASCII characters).
- **component-id**—The ID of the component reporting the event or alarm (1 to 32 ASCII characters).
Specifying the component-ID, setting type to a value, and specifying a number displays only alarms of that type and number from the designated component.
- **start-time** or **end-time**—The timestamp indicating the time interval for reporting events or alarms in the format <yyyy-mm-dd hh:mm:ss> where:
 - yyyy—year (4-digit number)
 - mm—month (01 to 12)
 - dd—day (01 to 31)
 - hh—hour (00 to 23)
 - mm—minute (00 to 59)
 - ss—second (00 to 59)

Show, Add, and Delete Event Queue Commands

The **event-queue** commands allow showing, adding, or deleting an event queue on a Call Agent or Feature Server.

```
show event-queue instance=CA146
add event-queue instance=CA146
delete event-queue instance=CA146
```

The **event-queue** commands must include the mandatory **instance** token, which specifies the Call Agent or Feature Server (CA nnn , Feature Server for POTS, Tandem, and Centrex services (FSPTC), Feature Server for AIN services (FSAIN)) where the event queue is located. Only one instance can be shown, added, or deleted at a time.

Saving Events to Log Files

Use the commands in this section to manage the way events and alarms are saved to their respective logs.

Show Report-Properties Command

Use the following **show report-properties** command to view the event or alarm properties currently used to specify which event levels, events, and alarms are saved to the event or alarm logs:

```
CLI>show report-properties
Reply: Success:  Entries 1-3 of 3 returned.

TYPE=EVENT_LOGSIZE
VALUE=30000

TYPE=ALARM_LOGSIZE
VALUE=30000

TYPE=EVENT_LEVEL
VALUE=INFO
```

**Note**

The **show report-properties** command, without any tokens, returns all alarm-logsize, event-logsize, and event-level data.

There are no mandatory tokens (parameters) required for the **show report-properties** command; however, you can optionally use the type and/or value tokens described below.

Changing Report Properties

Use the following **change report-properties** command to specify the maximum number and/or the severity of event or alarm entries to be saved to the event or alarm logs:

```
change report-properties type=<event-logsize|alarm-logsize>; value=<logsize>;
```

or

```
change report-properties type=<event-level>; value=<severity>
```

The **type** and **value** tokens are both mandatory for the **change report-properties** command.

- If type=event-logsize or alarm-logsize, then value must be an integer between 10 to 30000.
- If type=event-level, then value designates the severity of the events or alarms to include in the log files, which can be info, warning, minor, major, or critical.

All events or alarms whose severity is equal to or greater than the event level specified are included in the designated event or alarm log file.

For example:

If info is designated, all events or alarms are included in the designated event or alarm log file. If minor is designated, minor, major, and critical events or alarms are included in the designated event or alarm log file.



Tip

Cisco recommends that you store events of *all* severity levels in the event and alarm log files by entering **info** as the value in this command. This permits the operator to access all event and alarm reports.

Changing Threshold and Throttle Values

The threshold and throttle values used in event and alarm reporting are user-provisionable. You can use the following **show event-prov** command to display the current threshold and throttle values for any event or alarm message:

```
CLI>show event-prov type=callp; number=9;
```

```
Reply: Success: Entry 1 of 1 returned.
```

```
REPORTTYPE=2
REPORTNUMBER=9
REPORTDESCRIPTION=No Route Available for Carrier Dialed
THRESHLIM=100
THROTTLELIM=20
DW1NAME=Orig Type(Trunk or S
DW2NAME=Orig Sub or TG id
DW3NAME=Calling Party Number
DW4NAME=Called Party Number
DW5NAME=Carrier Code Dialed
DW6NAME=n/a
DW7NAME=n/a
DW8NAME=n/a
CAUSE1=No route is available for the interexchange carrier (IXC) dialed.
ACTION1=The data words in the event report indicate the parameters that need to be
corrected. Refer to office records for the carrier.
CAUSE2=Parameter(s) in the carrier and/or route-grp table are missing or incorrect for the
carrier.
ACTION2=Determine whether the routing parameters were entered correctly in the carrier
and/or route-grp tables.
ACTION3=If the carrier-id or route-grp-id are not specified, or are incorrect in the
dial-plan table, enter the correct values. Use the change carrier or change route-grp
command.
```

The command **show event-prov** with no parameters displays all events that are provisioned.

The command **show event-prov** with only **type** specified displays all events of that type.

Use the following **change event-prov** command to specify event threshold and throttle values other than the defaults:

```
change event-prov type=<type>; number=<n>; threshold=<n>; throttle=<n>;
```

- **threshold**—This value is the *maximum* number of reports of the event or alarm that can be reported in a 30-minute interval. Valid values are 0 to 100.
- **throttle**—This value is the number of occurrences of the designated event or alarm message required to trigger the issuance of one report. Valid values are 0 to 100.

The threshold to throttle ratio is used to limit how many entries of the same event/alarm occur within a 30 minute interval, i.e. if set 100/1 then for every 100 occurrences of an event only one entry is recorded in the log.

Managing and Responding to Events and Alarms

To manage and respond to events and alarms, complete the following steps:

- Step 1** Set the **event-logsize** and **event-level** parameters as desired using the **report-properties** command (see the [“Changing Report Properties”](#) section on page 1-15).
- Step 2** Subscribe to events and request event summary reports as needed using the **subscribe** command (see the [“Managing Event and Alarm Reports”](#) section on page 1-9).
- Step 3** Set the **alarm-logsize** and **event-level** parameters as desired using the **report-properties** command (see the [“Changing Report Properties”](#) section on page 1-15).
- Step 4** Subscribe to alarms and request alarm summary reports as needed using the **subscribe** command (see the [“Managing Event and Alarm Reports”](#) section on page 1-9).
- Step 5** Set the **threshold** and **throttle** parameters as desired using the **change event-prov** command (see the [“Changing Threshold and Throttle Values”](#) section on page 1-16).
- Step 6** View event and alarm reports and investigate potential problems.
Examples of problems to look for include: congestion warnings, routing errors, termination failures, billing errors, diagnostic failures, security warnings, and process failovers.
- Step 7** Refer to the “Probable Cause” and “Corrective Action” instructions for events and alarms in the [“Events and Alarms Descriptions and Corrective Actions”](#) section on page 1-18.
- Step 8** Take the necessary corrective action; escalate the problem if necessary.
The situation that caused an event or alarm must be resolved before the event or alarm can be cleared.
- Step 9** After the problem is fixed, enter the following command to clear a specific alarm:

```
clear alarm id=<sn>
```

Where:

ID is the system-assigned serial number of the event or alarm.



Note Clearing of an alarm but not the symptom will cause the alarm to reappear.

Events and Alarms Descriptions and Corrective Actions

This section describes all the events and alarms that are generated by the Cisco BTS 10200 Softswitch software. Each description includes the probable cause of the event or alarm and the corrective action that should be taken.

Format of Events and Alarms

System messages, informational events, and alarms reported by the Cisco BTS 10200 Softswitch are discussed in this section. Headings in left column (as shown in the following the example) and the type of information contained in the text in the right column adjacent to each of the headings are explained in the sections that follow.

SIGNALING (20) Example

DESCRIPTION	Link Set Congestion
SEVERITY	MAJOR
THRESHOLD	100
THROTTLE	0
DATAWORDS	Link Set No - ONE_BYTE Link Set Name - STRING [8] Congestion Level - ONE_BYTE
PRIMARY CAUSE	Issued when the specified SS7 link set is experiencing congestion.
PRIMARY ACTION	Monitor event reports at the network level to determine if the traffic load on the specified SS7 link set is too high on the local end, or if the remote end is lagging in processing the traffic.
SECONDARY ACTION	Verify that the SS7 link set has not degraded in quality.
TERNARY ACTION	Verify that the traffic load has not become unbalanced if multiple SS7 link sets are used.
SUBSEQUENT ACTION	Verify that local SS7 signaling adapter process is running normally.

Message Type and Number

The message type and number describe the type of alarm or event, the number assigned to the message, and the message text as it is displayed on the operator console or in a log file.

Cisco BTS 10200 Softswitch events and alarms are categorized into the following eleven types:

- **AUDIT**—Events or alarms generated by the audit subsystem. Refer to [Chapter 2, “Audit Troubleshooting.”](#)
- **BILLING**—Events or alarms generated by the billing subsystem. Refer to [Chapter 3, “Billing Troubleshooting.”](#)
- **CALLP**—Events or alarms generated by call processing. Refer to [Chapter 4, “Call Processing Troubleshooting.”](#)
- **CONFIG**—Events or alarms generated that provide information about system configuration. Refer to [Chapter 5, “Configuration Troubleshooting.”](#)
- **DATABASE**—Events or alarms generated by the database. Refer to [Chapter 6, “Database Troubleshooting.”](#)
- **MAINTENANCE**—Events or alarms that provide information about maintenance. Refer to [Chapter 7, “Maintenance Troubleshooting.”](#)
- **OSS**—Events or alarms generated by the OSS. Refer to [Chapter 8, “Operations Support System Troubleshooting.”](#)
- **SECURITY**—Events or alarms generated by the billing subsystem. Refer to [Chapter 9, “Security Troubleshooting.”](#)
- **SIGNALING**—Events or alarms generated by signaling protocols or interfaces. Refer to [Chapter 10, “Signaling Troubleshooting.”](#)
- **STATISTICS**—Events or alarms that provide information about system statistics. Refer to [Chapter 11, “Statistics Troubleshooting.”](#)
- **SYSTEM**—Events or alarms that convey information about system status or trouble. Refer to [Chapter 12, “System Troubleshooting.”](#)

Event Level

The event level designates the severity levels of the event or alarm information that is sent to the operator interface. Each event or alarm report is tagged with one of the following event level designations, listed from highest to lowest severity.

- **CRITICAL**—Service can be severely affected and an alarm is raised. A critical alarm indicates a critical situation exists somewhere in the system. Critical alarms can cause failovers (active server switches processing to standby server). Critical alarms must be investigated and cleared immediately.
- **MAJOR**—Service can be degraded and an alarm is raised. A major alarm indicates that a serious situation exists that can disrupt service. Major alarms differ from critical alarms in that they usually do not cause failovers. Major alarms should also be investigated and cleared immediately.
- **MINOR**—Service (call processing) is not affected; however, an alarm is raised. Minor alarms should be noted and cleared as soon as possible.
- **WARNING**—Warning messages provide cautionary advice about a potential service impact. They indicate conditions that should be investigated immediately to ensure that the situation does not progress into an alarmed state.

- **INFO**—Informational events indicate various stages of system operation as well as atypical network conditions, such as timer expirations, values that have exceeded preset thresholds, or unexpected responses from endpoints to signaling messages sent by the Cisco BTS 10200 Softswitch.

Under normal operating conditions, no alarms should occur. However, any alarms that do occur should be investigated immediately. It is normal for events of INFO and WARNING levels to occur; however, these events should also be reviewed promptly by the operator.

Threshold/Throttle

The threshold value can range and is configurable. Currently, when configuring the threshold via CLI or other various adapters, the maximum limit on the threshold is 100. However, there are ways of setting the threshold to over 100 that must be coordinated with Cisco Customer Support. Setting the threshold to anything over 100 can cause performance degradation to the system. There are some events that have threshold over 100 as defaults.



Note

To disable sending of a particular event or alarm, set the threshold to 0.

The threshold describes the maximum number of events or alarms sent within a 30 minute interval before the rest are discarded. For example, if the threshold is 50, then anything after the first 50 events of the same type and id are discarded after it has received 50 of those events or alarms within a 30 minute interval. After the 30 minute interval (on the hour) expires, the running threshold count is reset back to 0.

Thottle describes the number of events or alarms suppressed for every X number of events/alarms. For example, if the throttle is 10 for a particular event or alarm, then the 1st through the 9th event are discarded and the 10th event is transmitted. In other words, every X (throttle) will be transmitted and every event in between will be discarded. The only exception is when the throttle set to 0, which means there is no throttle and all events will be sent (up to the maximum threshold).

When combining threshold and throttle, only the transmitted event counts towards threshold count. For example, if threshold and throttle for an event is 30/10, respectively, then there can be 300 events that are issued. So the 10th, 20th, 30th, etc. events are sent and those sent events are counted toward the threshold count. The last event being sent is 300th.

Data Reported

Depending on the specific event or alarm being reported, additional data fields (parameters) can also be reported by the system. A single report can have as many as eight additional data fields. The length of a string is denoted by a number in parentheses (*n*). The length of other types of fields is denoted by the number of bytes in parentheses (*n* bytes).

Probable Cause

The probable cause contains descriptions of the network or system conditions causing the event or alarm. Where multiple causes are possible, each cause is numbered and described in the order of its relative probability.

Corrective Action

The corrective action contains recommendations for resolving the problem, if applicable. Where multiple actions are possible, each action is numbered and described in the order in which they should be performed.



CHAPTER 2

Audit Troubleshooting

Revised: October 23, 2008, OL-11335-06

Introduction

This chapter provides the information needed to monitor and troubleshoot Audit events and alarms. This chapter is divided into the following sections:

- [Audit Events and Alarms](#) – Provides a brief overview of each Audit event and alarm.
- [Monitoring Audit Events](#) – Provides the information needed to monitor and correct Audit events.
- [Troubleshooting Audit Alarms](#) – Provides the information needed to troubleshoot and correct Audit alarms.

Audit Events and Alarms

This section provides a brief overview of the Audit events and alarms for the Cisco BTS 10200 Softswitch in numerical order. [Table 2-1](#) lists all of the audit events and alarms by severity.


Note

Click the Audit message number in [Table 2-1](#) to display information about the event or alarm.

Table 2-1 **Audit Events and Alarms by Severity**

CRITICAL	MAJOR	MINOR	WARNING	INFO
AUDIT (5)	AUDIT (6)	AUDIT (7)	AUDIT (3)	AUDIT (1)
			AUDIT (4)	AUDIT (2)
			AUDIT (8)	

AUDIT (1)

For additional information, refer to the “[Test Report - Audit \(1\)](#)” section on page 2-6.

DESCRIPTION	Test Report
SEVERITY	Information (INFO)
THRESHOLD	100
THROTTLE	0
PRIMARY CAUSE	This event is used for testing the new “Audit” category.
PRIMARY ACTION	No action is necessary.

AUDIT (2)

For additional information, refer to the “[Start or Stop of Signaling System 7 - Circuit Identification Code Audit - Audit \(2\)](#)” section on page 2-6.

DESCRIPTION	Start or Stop of Signaling System 7-Circuit Identification Code Audit (Start or Stop of SS7-CIC Audit)
SEVERITY	INFO
THRESHOLD	100
THROTTLE	0
DATAWORDS	Type of Audit - STRING [64]
PRIMARY CAUSE	Signaling System 7 (SS7) circuit identification code (CIC) audit has started or stopped.
PRIMARY ACTION	No action required - normal operation.

AUDIT (3)

To monitor and correct the cause of the event, refer to the [“Signaling System 7 Circuit Identification Code Audit Terminated Before Successful Completion - Audit \(3\)”](#) section on page 2-6.

DESCRIPTION	Signaling System 7 Circuit Identification Code Audit Terminated Before Successful Completion (SS7 CIC Audit Terminated Before Successful Completion)
SEVERITY	WARNING
THRESHOLD	100
THROTTLE	0
DATAWORDS	Type of Audit - STRING [64]
PRIMARY CAUSE	A higher priority SS7 CIC audit interrupted and terminated a lower priority SS7 CIC audit.
PRIMARY ACTION	Do not schedule an SS7 remote termination audit to occur while a periodic SS7 local termination audit is executing.

AUDIT (4)

To monitor and correct the cause of the event, refer to the [“Call Exceeds a Long-Duration Threshold - Audit \(4\)”](#) section on page 2-7

DESCRIPTION	Call Exceeds a Long-Duration Threshold
SEVERITY	WARNING
THRESHOLD	100
THROTTLE	0
DATAWORDS	Trunk group number - TWO_BYTES Trunk member number - TWO_BYTES Current long-duration threshold - TWO_BYTES
PRIMARY CAUSE	Call exceeds current system long-duration threshold.
PRIMARY ACTION	If there is reason to believe the call is no longer valid, release the associated trunk facility.

AUDIT (5)

To troubleshoot and correct the cause of the alarm, refer to the [“Critical Internal Audit Failure - Audit \(5\)” section on page 2-9](#).

DESCRIPTION	Critical Internal Audit Failure
SEVERITY	CRITICAL
THRESHOLD	100
THROTTLE	0
DATAWORDS	Failure Details - STRING [220] Probable Causes - STRING [80] Corrective Actions - STRING [80]
PRIMARY CAUSE	See data field.
PRIMARY ACTION	See data field.

AUDIT (6)

To troubleshoot and correct the cause of the alarm, refer to the [“Major Internal Audit Failure - Audit \(6\)” section on page 2-9](#).

DESCRIPTION	Major Internal Audit Failure
SEVERITY	MAJOR
THRESHOLD	100
THROTTLE	0
DATAWORDS	Failure Details - STRING [220] Probable Causes - STRING [80] Corrective Actions - STRING [80]
PRIMARY CAUSE	See data field.
PRIMARY ACTION	See data field.

AUDIT (7)

To troubleshoot and correct the cause of the alarm, refer to the [“Minor Internal Audit Failure - Audit \(7\)” section on page 2-9](#).

DESCRIPTION	Minor Internal Audit Failure
SEVERITY	MINOR
THRESHOLD	100
THROTTLE	0
DATAWORDS	Failure Details - STRING [220] Probable Causes - STRING [80] Corrective Actions - STRING [80]
PRIMARY CAUSE	See data field.
PRIMARY ACTION	See data field.

AUDIT (8)

To monitor and correct the cause of the event, refer to the [“Warning From Internal Audit - Audit \(8\)” section on page 2-8](#).

DESCRIPTION	Warning From Internal Audit
SEVERITY	WARNING
THRESHOLD	100
THROTTLE	0
DATAWORDS	Failure Details - STRING [220] Probable Causes - STRING [80] Corrective Actions - STRING [80]
PRIMARY CAUSE	See data field.
PRIMARY ACTION	See data field.

Monitoring Audit Events

This section provides the information needed to monitor and correct Audit events. [Table 2-2](#) lists all Audit events in numerical order and provides cross reference to each subsection in this section.

Table 2-2 *Cisco BTS 10200 Softswitch Audit Events*

Event Type	Event Name	Event Severity
AUDIT(1)	Test Report - Audit (1)	INFO
AUDIT(2)	Start or Stop of Signaling System 7 - Circuit Identification Code Audit - Audit (2)	INFO
AUDIT(3)	Signaling System 7 Circuit Identification Code Audit Terminated Before Successful Completion - Audit (3)	WARNING
AUDIT(4)	Call Exceeds a Long-Duration Threshold - Audit (4)	WARNING
AUDIT(5)	Critical Internal Audit Failure - Audit (5)	CRITICAL
AUDIT(6)	Major Internal Audit Failure - Audit (6)	MAJOR
AUDIT(7)	Minor Internal Audit Failure - Audit (7)	MINOR
AUDIT(8)	Warning From Internal Audit - Audit (8)	WARNING

Test Report - Audit (1)

The Test Report event is used for testing the audit event category. The event is informational and no further action is required.

Start or Stop of Signaling System 7 - Circuit Identification Code Audit - Audit (2)

The Start or Stop of Signaling System 7 - Circuit Identification Code Audit event occurs as part of normal Cisco BTS 10200 Softswitch operation. The event is informational and no further action is required.

Signaling System 7 Circuit Identification Code Audit Terminated Before Successful Completion - Audit (3)

The Signaling System 7 Circuit Identification Code Audit Terminated Before Successful Completion event serves as a warning that a higher priority SS7 CIC audit has interrupted and terminated a lower priority SS7 CIC audit. To control the occurrence of this event an SS7 remote termination audit should not be scheduled to occur while a periodic SS7 local termination audit is executing.

Call Exceeds a Long-Duration Threshold - Audit (4)

The Call Exceeds a Long-Duration Threshold event serves as a warning that a call has exceeded the current the Cisco BTS 10200 Softswitch system long-duration threshold. If there is reason to believe the call is no longer valid, the associated trunk facility should be released.

To check the current threshold setting for Long Duration calls, proceed as follows:

Step 1 As root user from the Call Agent (CA), execute the following command:

```
# grep LongDuration /opt/OptiCall/`ls /opt/OptiCall | grep CA`/bin/platform.cfg
```

Step 2 Review the command results.

Example results:

```
Args=-ems_pri_dn blg-asys07EMS.mssol.cisco.com -ems_sec_dn blg-asys07EMS.mssol.cisco.com  
-port 15260  
-QCheckInterval1 1000 -QCheckInterval2 4500 -RecordGenTime 00:00:00 -LongDurationAllowance  
1440  
-QCheckInterval3 60 -MyCaBillingDn blg-asys07CA.mssol.cisco.com
```



Note

Following a platform start, the billing system will wait until the present time (current time on the call agent) is equal to RecordGenTime before auditing for Long Duration Calls. After the initial audit, the billing system will perform a Long Duration Call audit every LongDurationAllowance minutes. During an audit, the billing system will generate a Long Duration CDR for calls that have been active for LongDurationAllowance minutes.

Critical Internal Audit Failure - Audit (5)

The Critical Internal Audit Failure alarm (critical) indicates that a critical internal audit failure has occurred. To troubleshoot and correct the cause of the Critical Internal Audit Failure alarm, refer to the [“Critical Internal Audit Failure - Audit \(5\)” section on page 2-9](#).

Major Internal Audit Failure - Audit (6)

The Major Internal Audit Failure alarm (major) indicates that a major internal audit failure has occurred. To troubleshoot and correct the cause of the Major Internal Audit Failure alarm, refer to the [“Major Internal Audit Failure - Audit \(6\)” section on page 2-9](#).

Minor Internal Audit Failure - Audit (7)

The Minor Internal Audit Failure alarm (minor) indicates that a minor internal audit failure has occurred. To troubleshoot and correct the cause of the Minor Internal Audit Failure alarm, refer to the [“Minor Internal Audit Failure - Audit \(7\)” section on page 2-9](#).

Warning From Internal Audit - Audit (8)

The Warning From Internal Audit event serves as a warning that a problem with an internal audit has occurred. To correct the internal audit problem refer to the failure details (220), probable cause (80), and corrective actions (80) listed in the data field. Additionally, refer to the previous critical, major, and minor internal audit failure sections.

Troubleshooting Audit Alarms

This section provides the information needed to troubleshoot and correct Audit alarms. [Table 2-3](#) lists all Audit alarms in numerical order and provides cross reference to each subsection in this section.

Table 2-3 Cisco BTS 10200 Softswitch Audit Alarms

Alarm Type	Alarm Name	Alarm Severity
AUDIT(5)	Critical Internal Audit Failure - Audit (5)	CRITICAL
AUDIT(6)	Major Internal Audit Failure - Audit (6)	MAJOR
AUDIT(7)	Minor Internal Audit Failure - Audit (7)	MINOR

Critical Internal Audit Failure - Audit (5)

The Critical Internal Audit Failure alarm (critical) indicates that a critical internal audit failure has occurred. To find the probable causes of the alarm, review the data field “Failure Details” and “Probable Causes” datawords. For the corrective actions for the alarm, review the data field “Corrective Actions” dataword. Once the “Corrective Actions” dataword has been reviewed, proceed with the corrective actions listed.

Major Internal Audit Failure - Audit (6)

The Major Internal Audit Failure alarm (major) indicates that a major internal audit failure has occurred. To find the probable causes of the alarm, review the data field “Failure Details” and “Probable Causes” datawords. For the corrective actions for the alarm, review the data field “Corrective Actions” dataword. Once the “Corrective Actions” dataword has been reviewed, proceed with the corrective actions listed.

Minor Internal Audit Failure - Audit (7)

The Minor Internal Audit Failure alarm (minor) indicates that a minor internal audit failure has occurred. To find the probable causes of the alarm, review the data field “Failure Details” and “Probable Causes” datawords. For the corrective actions for the alarm, review the data field “Corrective Actions” dataword. Once the “Corrective Actions” dataword has been reviewed, proceed with the corrective actions listed.



CHAPTER 3

Billing Troubleshooting

Revised: October 23, 2008, OL-11335-06

Introduction

This chapter provides the information needed to monitor and troubleshoot Billing events and alarms. This chapter is divided into the following sections:

- [Billing Events and Alarms](#) – Provides a brief overview of each Billing event and alarm.
- [Monitoring Billing Events](#) – Provides the information needed to monitor and correct Billing events.
- [Troubleshooting Billing Alarms](#) – Provides the information needed to troubleshoot and correct Billing alarms.



Note

The following billing records are created when a call is rejected due to overload conditions:

- SS7 termination cause code 42
- Cable signaling stop event cause code “resource unavailable”

Calls rejected by the signaling adapter will not generate a billing record.

Billing Events and Alarms

This section provides a brief overview of the Billing events and alarms for the Cisco BTS 10200 Softswitch in numerical order. [Table 3-1](#) lists all of the billing events and alarms by severity.


Note

Click the Billing message number in [Table 3-1](#) to display information about the event or alarm.

Table 3-1 *Billing Events and Alarms by Severity*

CRITICAL	MAJOR	MINOR	WARNING	INFO
BILLING (4)	BILLING (3)	BILLING (2)	BILLING (14)	BILLING (1)
BILLING (7)	BILLING (6)	BILLING (39)	BILLING (42)	BILLING (5)
BILLING (13)	BILLING (8)	BILLING (40)		BILLING (36)
BILLING (35)	BILLING (15)	BILLING (41)		BILLING (57)
BILLING (49)	BILLING (29)	BILLING (45)		
BILLING (52)	BILLING (30)	BILLING (46)		
BILLING (55)	BILLING (31)	BILLING (47)		
BILLING (56)	BILLING (32)	BILLING (53)		
	BILLING (33)			
	BILLING (37)			
	BILLING (38)			
	BILLING (44)			
	BILLING (48)			
	BILLING (54)			
	BILLING (58)			

BILLING (1)

For additional information, refer to the “[Test Report - Billing \(1\)](#)” section on page 3-23.

DESCRIPTION	Test Report
SEVERITY	Information (INFO)
THRESHOLD	10000
THROTTLE	0

BILLING (2)

To troubleshoot and correct the cause of the alarm, refer to the [“Billing Partition Disk Usage Minor Threshold Exceeded - Billing \(2\)”](#) section on page 3-31.

DESCRIPTION	Billing Partition Disk Usage Minor Threshold Exceeded
SEVERITY	MINOR
THRESHOLD	100
THROTTLE	0
DATAWORDS	Disk Usage Percentage - TWO_BYTES
PRIMARY CAUSE	Call detail records are accumulating on the disk associated with the billing database in the Element Management System (EMS). This is because data is being written into the database faster than it is being read out of the database. The minor threshold (default value = 70%) has been exceeded.
PRIMARY ACTION	Monitor this alarm. The read should catch up to write within a few minutes, and the alarm should not remain active.
SECONDARY CAUSE	Some fluctuation in disk usage is to be expected as call volume rises and falls during the day. Threshold crossings might step upward (from MINOR to MAJOR to CRITICAL) when there is a rapid increase in call volume, and then step downward (CRITICAL to MAJOR to MINOR) when call volume slows.
SECONDARY ACTION	To monitor the alarm, use the subscribe alarm-report command. To obtain a summary, use the report alarm-summary command. Verify that type = billing is entered in these commands.

BILLING (3)

To troubleshoot and correct the cause of the alarm, refer to the [“Billing Partition Disk Usage Major Threshold Exceeded - Billing \(3\)”](#) section on page 3-31.

DESCRIPTION	Billing Partition Disk Usage Major Threshold Exceeded
SEVERITY	MAJOR
THRESHOLD	100
THROTTLE	0
DATAWORDS	Disk Usage Percentage - TWO_BYTES
PRIMARY CAUSE	Call detail records are accumulating on the disk associated with the billing database in the EMS. This is because data is being written into the database faster than it is being read out of the database. The major threshold (default value = 80%) has been exceeded.
PRIMARY ACTION	Monitor this alarm. The read should catch up to write within a few minutes, and the alarm should not remain active.
SECONDARY CAUSE	Some fluctuation in disk usage is to be expected as call volume rises and falls during the day. Threshold crossings might step upward (from MINOR to MAJOR to CRITICAL) when there is a rapid increase in call volume, and then step downward (CRITICAL to MAJOR to MINOR) when call volume slows.
SECONDARY ACTION	To monitor the alarm, use the subscribe alarm-report command. To obtain a summary, use the report alarm-summary command. Verify that type = billing is entered in these commands.
TERNARY ACTION	If the alarm does not clear (or step down to a reduced level) in a few minutes, contact Cisco Technical Assistance Center (TAC) for assistance.

Refer to the [“Obtaining Technical Assistance”](#) section on page xxxviii for detailed instructions on contacting Cisco TAC and opening a service request.

BILLING (4)

To troubleshoot and correct the cause of the alarm, refer to the [“Billing Partition Disk Usage Critical Threshold Exceeded - Billing \(4\)”](#) section on page 3-31.

DESCRIPTION	Billing Partition Disk Usage Critical Threshold Exceeded
SEVERITY	CRITICAL
THRESHOLD	100
THROTTLE	0
DATAWORDS	Disk Usage Percentage - TWO_BYTES
PRIMARY CAUSE	Call detail records are accumulating on the disk associated with the billing database in the EMS. This is because data is being written into the database faster than it is being read out of the database. The major threshold (default value = 90%) has been exceeded.
PRIMARY ACTION	Monitor this alarm. The read should catch up to write within a few minutes, and the alarm should not remain active.
SECONDARY CAUSE	Some fluctuation in disk usage is to be expected as call volume rises and falls during the day. Threshold crossings might step upward (from MINOR to MAJOR to CRITICAL) when there is a rapid increase in call volume, and then step downward (CRITICAL to MAJOR to MINOR) when call volume slows.
SECONDARY ACTION	To monitor the alarm, use the subscribe alarm-report command. To obtain a summary, use the report alarm-summary command. Verify that type = billing is entered in these commands.
TERNARY ACTION	If the alarm does not clear (or step down to a reduced level) in a few minutes, contact Cisco TAC for assistance.

Refer to the [“Obtaining Technical Assistance”](#) section on page xxxviii for detailed instructions on contacting Cisco TAC and opening a service request.

BILLING (5)

For additional information, refer to the [“Billing Partition Disk Usage Within Normal Range - Billing \(5\)”](#) section on page 3-23.

DESCRIPTION	Billing Partition Disk Usage Within Normal Range
SEVERITY	INFO
THRESHOLD	100
THROTTLE	0
DATAWORDS	Disk Usage Percentage - TWO_BYTES

BILLING (6)

To troubleshoot and correct the cause of the alarm, refer to the [“File Transfer Protocol/Secure File Transfer Protocol Transfer Failed - Billing \(6\)”](#) section on page 3-32.


Note

OpenSSH version 3.9p1 contains a bug that may cause billing file transfers over SFTP to fail.

DESCRIPTION	File Transfer Protocol/Secure File Transfer Protocol Transfer Failed (FTP/SFTP Transfer Failed)
SEVERITY	MAJOR
THRESHOLD	100
THROTTLE	0
DATAWORDS	TransferType - STRING [5] FileName - STRING [40] RemoteAddress - STRING [40] Error - STRING [50]
PRIMARY CAUSE	Unable to connect to remote host.
PRIMARY ACTION	Verify the remote host is reachable. Run “show billing-acct-addr” and verify billing-server-addr is correct. Change billing-server-addr, if necessary, via “change billing-acct-addr”.
SECONDARY CAUSE	Unable to login to remote host.
SECONDARY ACTION	Use “show billing-acct-addr” to verify user-name is a valid user for the host specified in billing-server-addr. If user-name is correct and the “TransferType” dataword shows “File Transfer Protocol (FTP)”, re-enter the password via “change billing-acct-addr”. If user-name is correct and the “TransferType” dataword shows “Secure File Transfer Protocol (SFTP)”, verify that secure shell (SSH) keys have been pre-configured for user-name on both the Cisco BTS 10200 Softswitch and the remote host.
TERNARY CAUSE	File transfer error.
TERNARY ACTION	Check the “Error” dataword to see if it gives an indication of the kind of error that occurred. It could be a file-system error on the remote host, or a communication failure between the Cisco BTS 10200 Softswitch and the remote host.

BILLING (7)

To troubleshoot and correct the cause of the alarm, refer to the [“Transmission Control Protocol Connection Error - Billing \(7\)” section on page 3-33](#).

DESCRIPTION	Transmission Control Protocol Connection Error (TCP Connection Error)
SEVERITY	CRITICAL
THRESHOLD	100
THROTTLE	0
DATAWORDS	Hostname - STRING [100]
PRIMARY CAUSE	System call error.
PRIMARY ACTION	Check address in platform configuration.
SECONDARY CAUSE	Not connected to the right address.
SECONDARY ACTION	Call Cisco TAC technical support. (Contact Cisco TAC.)

Refer to the [“Obtaining Technical Assistance” section on page xxxviii](#) for detailed instructions on contacting Cisco TAC and opening a service request.

BILLING (8)

To troubleshoot and correct the cause of the alarm, refer to the [“Transmission Control Protocol Packet Receive Failure - Billing \(8\)” section on page 3-33](#).

DESCRIPTION	Transmission Control Protocol Packet Receive Failure (TCP Packet Receive Failure)
SEVERITY	MAJOR
THRESHOLD	100
THROTTLE	0
DATAWORDS	Host Name - STRING [25]
PRIMARY CAUSE	Peer went down; socket closed.
PRIMARY ACTION	Check the peer’s status and bring it up.



Note

BILLING (9) through BILLING (12) are not used.

BILLING (13)

To troubleshoot and correct the cause of the alarm, refer to the [“Database Connection Error - Billing \(13\)” section on page 3-33](#).

DESCRIPTION	Database Connection Error
SEVERITY	CRITICAL
THRESHOLD	100
THROTTLE	0
PRIMARY CAUSE	Structured Query Language (SQL) server is down.
PRIMARY ACTION	Restart server; if this does not correct the problem, call Cisco TAC technical support. (Contact Cisco TAC.)

Refer to the [“Obtaining Technical Assistance” section on page xxxviii](#) for detailed instructions on contacting Cisco TAC and opening a service request.

BILLING (14)

To monitor and correct the cause of the event, refer to the [“File Open Error - Billing \(14\)” section on page 3-24](#).

DESCRIPTION	File Open Error
SEVERITY	WARNING
THRESHOLD	100
THROTTLE	0
DATAWORDS	Path Name - STRING [100]
PRIMARY CAUSE	System error, may be out of file descriptors.
PRIMARY ACTION	Call Cisco TAC technical support. (Contact Cisco TAC.)

Refer to the [“Obtaining Technical Assistance” section on page xxxviii](#) for detailed instructions on contacting Cisco TAC and opening a service request.

BILLING (15)

To troubleshoot and correct the cause of the alarm, refer to the [“File Write Error - Billing \(15\)”](#) section on page 3-33.

DESCRIPTION	File Write Error
SEVERITY	MAJOR
THRESHOLD	100
THROTTLE	0
DATAWORDS	Path Name - STRING [100]
PRIMARY CAUSE	System error, may be out of file descriptors.
PRIMARY ACTION	Call Cisco TAC technical support. (Contact Cisco TAC.)

Refer to the [“Obtaining Technical Assistance”](#) section on page xxxviii for detailed instructions on contacting Cisco TAC and opening a service request.



Note

BILLING (16) through BILLING (28) are not used.

BILLING (29)

To troubleshoot and correct the cause of the alarm, refer to the [“Call Data Block Send Failed - Billing \(29\)”](#) section on page 3-33.

DESCRIPTION	Call Data Block Send Failed (CDB Send Failed)
SEVERITY	MAJOR
THRESHOLD	100
THROTTLE	0
PRIMARY CAUSE	Transmission Control Protocol (TCP) send call failure.
PRIMARY ACTION	Check the port number and address of the blg and bmg processes in the platform.cfg file.
SECONDARY CAUSE	Both the EMS servers are down.
SECONDARY ACTION	Check if both EMS servers are down. If so, bring at least one up.

BILLING (30)

To troubleshoot and correct the cause of the alarm, refer to the [“Domain Name Mapping Failed - Billing \(30\)” section on page 3-34](#).

DESCRIPTION	Domain Name Mapping Failed
SEVERITY	MAJOR
THRESHOLD	100
THROTTLE	0
DATAWORDS	Address - STRING [50]
PRIMARY CAUSE	Wrong domain name system (DNS) name mapping specified in the configuration files.
PRIMARY ACTION	Check the optcall.cfg and platform.cfg for the right mapping.

BILLING (31)

To troubleshoot and correct the cause of the alarm, refer to the [“Port not Specified - Billing \(31\)” section on page 3-34](#).

DESCRIPTION	Port not Specified
SEVERITY	MAJOR
THRESHOLD	100
THROTTLE	0
PRIMARY CAUSE	Port not specified in the platform.cfg file.
PRIMARY ACTION	Check platform.cfg file and add the argument to blg -port 15260.

BILLING (32)

To troubleshoot and correct the cause of the alarm, refer to the [“Element Management System Address not Specified - Billing \(32\)” section on page 3-34](#).

DESCRIPTION	Element Management System Address not Specified (EMS Address not Specified)
SEVERITY	MAJOR
THRESHOLD	100
THROTTLE	0
PRIMARY CAUSE	Either the primary or secondary EMS address has not been specified in the platform.cfg file.
PRIMARY ACTION	Check the platform.cfg for the process billing (BLG) and add the missing addresses to the file.

BILLING (33)

To troubleshoot and correct the cause of the alarm, refer to the [“File Transfer Protocol/Secure File Transfer Protocol Parameters Invalid - Billing \(33\)”](#) section on page 3-34.

DESCRIPTION	File Transfer Protocol/Secure File Transfer Protocol Parameters Invalid (FTP/SFTP Parameters Invalid)
SEVERITY	MAJOR
THRESHOLD	100
THROTTLE	0
DATAWORDS	TransferType - STRING [5] BillingServerDir - STRING [100] BillingServerAddr - STRING [100] User Name - STRING [100]
PRIMARY CAUSE	The billing-acct-addr table is not fully provisioned with the information needed to perform file transfers.
PRIMARY ACTION	Check billing-acct-addr fields via “show billing-acct-addr”. For FTP file transfer, ensure billing-server-addr, billing-server-directory, user-name, and password (not displayed) are provisioned. Also ensure sftp-supp is set to “N”. For SFTP file transfer, ensure billing-server-addr, billing-server-directory, and user-name are provisioned. Also ensure sftp-supp is set to “Y”.



Note

BILLING (34) is not used.

BILLING (35)

To troubleshoot and correct the cause of the alarm, refer to the [“All Billing Links at Billing Server Down - Billing \(35\)”](#) section on page 3-34.

DESCRIPTION	All Billing Links at Billing Server Down
SEVERITY	CRITICAL
THRESHOLD	100
THROTTLE	0
PRIMARY CAUSE	Cable connection might have been pulled out.
PRIMARY ACTION	Restore the cable connection.
SECONDARY CAUSE	An “ifconfig down” might have been done on the interfaces.
SECONDARY ACTION	Execute a “ifconfig up”.

BILLING (36)

For additional information, refer to the [“Billing Link Restored - Billing \(36\)”](#) section on page 3-26.

DESCRIPTION	Billing Link Restored
SEVERITY	INFO
THRESHOLD	100
THROTTLE	0
DATAWORDS	Interface Name - STRING [50]
PRIMARY CAUSE	Cable has been restored.
PRIMARY ACTION	None

BILLING (37)

To troubleshoot and correct the cause of the alarm, refer to the [“Billing Link Failure - Billing \(37\)”](#) section on page 3-35.

DESCRIPTION	Billing Link Failure
SEVERITY	MAJOR
THRESHOLD	100
THROTTLE	0
DATAWORDS	Interface Name - STRING [5]
PRIMARY CAUSE	Cable may have been pulled.
PRIMARY ACTION	Restore cable connection.
SECONDARY CAUSE	An “ifconfig down” may have been performed on the interface.
SECONDARY ACTION	Perform an “ifconfig up” on the interface.

BILLING (38)

To troubleshoot and correct the cause of the alarm, refer to the [“Event Message Log File Access Error - Billing \(38\)” section on page 3-35](#).

DESCRIPTION	Event Message Log File Access Error (EM Log File Access Error)
SEVERITY	MAJOR
THRESHOLD	50
THROTTLE	0
DATAWORDS	Type of Access Error - STRING [25] Reason for Error - STRING [40] Sequence Number OFF - FOUR_BYTES Index of Event Messa - FOUR_BYTES Location Tag - STRING [30]
PRIMARY CAUSE	System error--may be out of file descriptors.
PRIMARY ACTION	Call Cisco TAC. (Contact Cisco TAC.)
SECONDARY CAUSE	Disk may be faulty.
SECONDARY ACTION	Cause the Bulk Data Management System (BDMS) to switch over to its mate node.

Refer to the [“Obtaining Technical Assistance” section on page xxxviii](#) for detailed instructions on contacting Cisco TAC and opening a service request.

BILLING (39)

To troubleshoot and correct the cause of the alarm, refer to the [“RADIUS Accounting Receive Failure - Billing \(39\)” section on page 3-35](#).

DESCRIPTION	RADIUS Accounting Receive Failure
SEVERITY	MINOR
THRESHOLD	25
THROTTLE	0
DATAWORDS	Location tag - STRING [30]
PRIMARY CAUSE	System error.
PRIMARY ACTION	If problem persists, call Cisco TAC. (Contact Cisco TAC.)

Refer to the [“Obtaining Technical Assistance” section on page xxxviii](#) for detailed instructions on contacting Cisco TAC and opening a service request.

BILLING (40)

To troubleshoot and correct the cause of the alarm, refer to the [“Event Message Encode Failure - Billing \(40\)” section on page 3-35](#).

DESCRIPTION	Event Message Encode Failure (EM Encode Failure)
SEVERITY	MINOR
THRESHOLD	100
THROTTLE	0
DATAWORDS	Location Tag - STRING [30]
PRIMARY CAUSE	There is a problem with the format of the data to be sent to the record keeping system (RKS).
PRIMARY ACTION	If problem persists, call Cisco TAC. (Contact Cisco TAC.)

Refer to the [“Obtaining Technical Assistance” section on page xxxviii](#) for detailed instructions on contacting Cisco TAC and opening a service request.

BILLING (41)

To troubleshoot and correct the cause of the alarm, refer to the [“Message Content Error - Billing \(41\)” section on page 3-35](#).

DESCRIPTION	Message Content Error
SEVERITY	MINOR
THRESHOLD	100
THROTTLE	0
DATAWORDS	Message Type - FOUR_BYTES Field Name - STRING [20] Field Value (Text) - STRING [20] Field Value (Numeric) - FOUR_BYTES Location Tag - STRING [30]
PRIMARY CAUSE	There is a mismatch between what the sender populated in the message and what the receiver expects.
PRIMARY ACTION	Call Cisco TAC. (Contact Cisco TAC.)

Refer to the [“Obtaining Technical Assistance” section on page xxxviii](#) for detailed instructions on contacting Cisco TAC and opening a service request.

BILLING (42)

To monitor and correct the cause of the event, refer to the [“Error Reading Provisioned Data–Using Default - Billing \(42\)” section on page 3-26](#).

DESCRIPTION	Error Reading Provisioned Data–Using Default
SEVERITY	WARNING
THRESHOLD	100
THROTTLE	0
DATAWORDS	Error Code - FOUR_BYTES Table Name - STRING [20] Field Name - STRING [20] Default Value (Decim - FOUR_BYTES Default Value (Text) - STRING [20] Location Tag - STRING [30]
PRIMARY CAUSE	Application was unable to read provisioned data, and had to resort to using default values.
PRIMARY ACTION	Check to ensure a complete load has been installed on the system. If load is complete and problem persists, call Cisco TAC. (Contact Cisco TAC.)

Refer to the [“Obtaining Technical Assistance” section on page xxxviii](#) for detailed instructions on contacting Cisco TAC and opening a service request.



Note

BILLING (43) is not used.

BILLING (44)

To troubleshoot and correct the cause of the alarm, refer to the [“Record Keeping System Switch Occurred - Billing \(44\)” section on page 3-36](#).

DESCRIPTION	Record Keeping System Switch Occurred (RKS Switch Occurred)
SEVERITY	MAJOR
THRESHOLD	100
THROTTLE	0
DATAWORDS	Type of RKS Switch - STRING [20] Location Tag - STRING [30]
PRIMARY CAUSE	Billing changed the destination RKS for transmitting event messages. The change could have been triggered by a communication problem with an RKS, or by an attempt to reestablish RKS communication.
PRIMARY ACTION	No action is necessary.

BILLING (45)

To troubleshoot and correct the cause of the alarm, refer to the [“Event Message Log File Opened - Billing \(45\)” section on page 3-36](#).

DESCRIPTION	Event Message Log File Opened
SEVERITY	MINOR
THRESHOLD	50
THROTTLE	0
DATAWORDS	Element Type - STRING [5] File Name - STRING [60] Location Tag - STRING [30]
PRIMARY CAUSE	A log file has been created for the storage of event messages that cannot be transmitted to an RKS.
PRIMARY ACTION	No action is necessary.

BILLING (46)

To troubleshoot and correct the cause of the alarm, refer to the [“Event Message Log File Closed - Billing \(46\)” section on page 3-36](#).

DESCRIPTION	Event Message Log File Closed
SEVERITY	MINOR
THRESHOLD	50
THROTTLE	0
DATAWORDS	Element Type - STRING [5] File Name - STRING [60] Location Tag - STRING [30]
PRIMARY CAUSE	An open event message log file has been closed.
PRIMARY ACTION	No action is necessary.

BILLING (47)

To troubleshoot and correct the cause of the alarm, refer to the [“Record Keeping System Unreachable for One Hour - Billing \(47\)”](#) section on page 3-36.

DESCRIPTION	Record Keeping System Unreachable for One Hour (RKSs Unreachable for 1 Hour)
SEVERITY	MINOR
THRESHOLD	25
THROTTLE	0
DATAWORDS	Location Tag - STRING [30]
PRIMARY CAUSE	Billing has not been able to communicate with any RKS for the past one hour.
PRIMARY ACTION	Check status of the primary and secondary RKS servers; attempt to bring them into service. Verify the radius-profile table and call-agent-profile table are provisioned such that communication with the RKS servers is possible.

BILLING (48)

To troubleshoot and correct the cause of the alarm, refer to the [“Record Keeping System Unreachable for Three Hours - Billing \(48\)”](#) section on page 3-36.

DESCRIPTION	Record Keeping System Unreachable for Three Hours (RKSs Unreachable for 3 Hours)
SEVERITY	MAJOR
THRESHOLD	25
THROTTLE	0
DATAWORDS	Location Tag - STRING [30]
PRIMARY CAUSE	Billing has not been able to communicate with any RKS for the past three hours.
PRIMARY ACTION	Check status of the primary and secondary RKS servers; attempt to bring them into service. Verify the radius-profile table and call-agent-profile table are provisioned such that communication with the RKS servers is possible.

BILLING (49)

To troubleshoot and correct the cause of the alarm, refer to the [“Record Keeping System Unreachable for 5 Hours - Billing \(49\)”](#) section on page 3-37.

DESCRIPTION	Record Keeping System Unreachable for 5 Hours (RKSs Unreachable for 5 Hours)
SEVERITY	CRITICAL
THRESHOLD	25
THROTTLE	0
DATAWORDS	Location Tag - STRING [30]
PRIMARY CAUSE	Billing has not been able to communicate with any RKS for the past five hours.
PRIMARY ACTION	Check status of the primary and secondary RKS servers; attempt to bring them into service. Verify the radius-profile table and call-agent-profile table are provisioned such that communication with the RKS servers is possible.



Note

BILLING (51) and BILLING (52) are not used.

BILLING (52)

To troubleshoot and correct the cause of the alarm, refer to the [“Bulk Data Management System Stopped Generating New Billing File - Billing \(52\)”](#) section on page 3-37.

DESCRIPTION	Bulk Data Management System Stopped Generating New Billing File (BDMS Stopped Generating New Billing File)
SEVERITY	CRITICAL
THRESHOLD	100
THROTTLE	0
PRIMARY CAUSE	Call detail records are accumulating on the disk associated with the billing files in the EMS. This is because data is being written into the billing files faster than it is being forwarded to the Billing Mediation Server. FTP to the Billing Mediation Server may not be working. The maximum disk partition for billing has been exceeded or the maximum number of files has been exceeded.
PRIMARY ACTION	Check Billing Mediation Server node name, user name and password specified in BILLING_ACCT_ADDR table and log files. Correct any error to let FTP start again. If billing_server_directory = "/dev/null" as in the lab, primary files under billing_directory will not be forwarded or deleted automatically. In this case, files have to be manually deleted or moved out, and BDMS needs to be restarted before it start generating new billing files.

BILLING (53)

To troubleshoot and correct the cause of the alarm, refer to the [“Event Message Disk Space 50 Percent Full - Billing \(53\)” section on page 3-37](#).

DESCRIPTION	Event Message Disk Space 50 Percent Full
SEVERITY	MINOR
THRESHOLD	100
THROTTLE	0
DATAWORDS	Number of Megabytes Used for Eve - FOUR_BYTES Directory Containing Event Messa - STRING [30] Location Tag - STRING [30]
PRIMARY CAUSE	Event message storage has reached 50% of the maximum storage allowed.
PRIMARY ACTION	Move event message files out of the specified directory. Store them in another location, or discard them.

BILLING (54)

To troubleshoot and correct the cause of the alarm, refer to the [“Event Message Disk Space 70 Percent Full - Billing \(54\)” section on page 3-37](#).

DESCRIPTION	Event Message Disk Space 70 Percent Full
SEVERITY	MAJOR
THRESHOLD	100
THROTTLE	0
DATAWORDS	Number of Megabytes Used for Eve - FOUR_BYTES Directory Containing Event Messa - STRING [30] Location Tag - STRING [30]
PRIMARY CAUSE	Event message storage has reached 70% of the maximum storage allowed.
PRIMARY ACTION	Move event message files out of the specified directory. Store them in another location, or discard them.

BILLING (55)

To troubleshoot and correct the cause of the alarm, refer to the [“Event Message Disk Space 100 Percent Full - Billing \(55\)” section on page 3-37](#).

DESCRIPTION	Event Message Disk Space 100 Percent Full
SEVERITY	CRITICAL
THRESHOLD	100
THROTTLE	0
DATAWORDS	Number of Megabytes Used for Eve - FOUR_BYTES Directory Containing Event Messa - STRING [30] Location Tag - STRING [30]
PRIMARY CAUSE	Event message storage has been completely filled. No additional event messages will be written to disk until more space is made available.
PRIMARY ACTION	Move event message files out of the specified directory. Store them in another location, or discard them.

BILLING (56)

To troubleshoot and correct the cause of the alarm, refer to the [“Billing Data Corruption Detected - Billing \(56\)” section on page 3-38](#).

DESCRIPTION	Billing Data Corruption Detected
SEVERITY	CRITICAL
THRESHOLD	100
THROTTLE	0
DATAWORDS	File/Table That May be Corrupt - STRING [32] Low End of the Range of Records - FOUR_BYTES High End of the Range of Records - FOUR_BYTES Error Code - FOUR_BYTES Location Tag - STRING [32]
PRIMARY CAUSE	Billing data stored on disk may have become corrupted due to a power outage, ungraceful shutdown, or disk failure.
PRIMARY ACTION	The BDMS that detected the problem should have gone out of service; leave it in the out-of-service state and contact Cisco TAC for assistance. (Contact Cisco TAC.)

Refer to the [“Obtaining Technical Assistance” section on page xxxviii](#) for detailed instructions on contacting Cisco TAC and opening a service request.

BILLING (57)

For additional information, refer to the [“Prepaid Subscriber Call Attempt Failed Because of Balance - Billing \(57\)” section on page 3-28.](#)

DESCRIPTION	Prepaid Subscriber Call Attempt Failed Because of Balance
SEVERITY	INFO
THRESHOLD	100
THROTTLE	0
DATAWORDS	Instance Name - STRING [65] Calling Party - STRING [32] Called Party - STRING [32] Pop ID- STRING [32]
PRIMARY CAUSE	Subscriber has run out of the balance.
PRIMARY ACTION	Ask the subscriber to deposit money in the account.
SECONDARY CAUSE	There may be a problem in billing info at prepaid server.
SECONDARY ACTION	Verify billing info at the prepaid server.

BILLING (58)

To troubleshoot and correct the cause of the alarm, refer to the [“Signaling Prepaid Server Inaccessible - Billing \(58\)” section on page 3-38.](#)

DESCRIPTION	Signaling Prepaid Server Inaccessible
SEVERITY	MAJOR
THRESHOLD	100
THROTTLE	0
DATAWORDS	Instance Name - STRING [65] Pop ID - STRING [32] Radius Profile ID - STRING [32]
PRIMARY CAUSE	All the prepaid servers are down.
PRIMARY ACTION	Check the operating status of prepaid servers.
SECONDARY CAUSE	Internet Protocol (IP) network between Cisco BTS 10200 Softswitch plain old telephone service (POTS) Feature Server (FS) and the prepaid servers is down.
SECONDARY ACTION	Check and correct any problems in IP network.

Monitoring Billing Events

This section provides the information needed to monitor and correct Billing events. [Table 3-2](#) lists all Billing events in numerical order and provides cross reference to each subsection in this section.

Table 3-2 *Cisco BTS 10200 Softswitch Billing Events*

Event Type	Event Name	Event Severity
BILLING(1)	Test Report - Billing (1)	INFO
BILLING(2)	Billing Partition Disk Usage Minor Threshold Exceeded - Billing (2)	MINOR
BILLING(3)	Billing Partition Disk Usage Major Threshold Exceeded - Billing (3)	MAJOR
BILLING(4)	Billing Partition Disk Usage Critical Threshold Exceeded - Billing (4)	CRITICAL
BILLING(5)	Billing Partition Disk Usage Within Normal Range - Billing (5)	INFO
BILLING(6)	File Transfer Protocol/Secure File Transfer Protocol Transfer Failed - Billing (6)	MAJOR
BILLING(7)	Transmission Control Protocol Connection Error - Billing (7)	CRITICAL
BILLING(8)	Transmission Control Protocol Packet Receive Failure - Billing (8)	MAJOR
BILLING(13)	Database Connection Error - Billing (13)	CRITICAL
BILLING(14)	File Open Error - Billing (14)	WARNING
BILLING(15)	File Write Error - Billing (15)	MAJOR
BILLING(29)	Call Data Block Send Failed - Billing (29)	MAJOR
BILLING(30)	Domain Name Mapping Failed - Billing (30)	MAJOR
BILLING(31)	Port not Specified - Billing (31)	MAJOR
BILLING(32)	Element Management System Address not Specified - Billing (32)	MAJOR
BILLING(33)	File Transfer Protocol/Secure File Transfer Protocol Parameters Invalid - Billing (33)	MAJOR
BILLING(35)	All Billing Links at Billing Server Down - Billing (35)	CRITICAL
BILLING(36)	Billing Link Restored - Billing (36)	INFO
BILLING(37)	Billing Link Failure - Billing (37)	MAJOR
BILLING(38)	Event Message Log File Access Error - Billing (38)	MAJOR
BILLING(39)	RADIUS Accounting Receive Failure - Billing (39)	MINOR
BILLING(40)	Event Message Encode Failure - Billing (40)	MINOR
BILLING(41)	Message Content Error - Billing (41)	MINOR
BILLING(42)	Error Reading Provisioned Data—Using Default - Billing (42)	WARNING
BILLING(44)	Record Keeping System Switch Occurred - Billing (44)	MAJOR
BILLING(45)	Event Message Log File Opened - Billing (45)	MINOR
BILLING(46)	Event Message Log File Closed - Billing (46)	MINOR
BILLING(47)	Record Keeping System Unreachable for One Hour - Billing (47)	MINOR
BILLING(48)	Record Keeping System Unreachable for Three Hours - Billing (48)	MAJOR
BILLING(49)	Record Keeping System Unreachable for Five Hours - Billing (49)	CRITICAL
BILLING(52)	Bulk Data Management System Stopped Generating New Billing File - Billing (52)	CRITICAL
BILLING(53)	Event Message Disk Space 50 Percent Full - Billing (53)	MINOR

Table 3-2 Cisco BTS 10200 Softswitch Billing Events (continued)

Event Type	Event Name	Event Severity
BILLING(54)	Event Message Disk Space 70 Percent Full - Billing (54)	MAJOR
BILLING(55)	Event Message Disk Space 100 Percent Full - Billing (55)	CRITICAL
BILLING(56)	Billing Data Corruption Detected - Billing (56)	CRITICAL
BILLING(57)	Prepaid Subscriber Call Attempt Failed Because of Balance - Billing (57)	INFO
BILLING(58)	Signaling Prepaid Server Inaccessible - Billing (58)	MAJOR

Test Report - Billing (1)

The Test Report event is used for testing the billing event category. The event is informational and no further action is required.

Billing Partition Disk Usage Minor Threshold Exceeded - Billing (2)

The Billing Partition Disk Usage Minor Threshold Exceeded alarm (minor) indicates that a billing partition disk usage minor threshold crossing has occurred. To troubleshoot and correct the cause of the Billing Partition Disk Usage Minor Threshold Exceeded alarm, refer to the [“Billing Partition Disk Usage Minor Threshold Exceeded - Billing \(2\)”](#) section on page 3-31.

Billing Partition Disk Usage Major Threshold Exceeded - Billing (3)

The Billing Partition Disk Usage Major Threshold Exceeded alarm (major) indicates that a billing partition disk usage major threshold crossing has occurred. To troubleshoot and correct the cause of the Billing Partition Disk Usage Major Threshold Exceeded alarm, refer to the [“Billing Partition Disk Usage Major Threshold Exceeded - Billing \(3\)”](#) section on page 3-31.

Billing Partition Disk Usage Critical Threshold Exceeded - Billing (4)

The Billing Partition Disk Usage Critical Threshold Exceeded alarm (critical) indicates that a billing partition disk usage critical threshold crossing has occurred. To troubleshoot and correct the cause of the Billing Partition Disk Usage Critical Threshold Exceeded alarm, refer to the [“Billing Partition Disk Usage Critical Threshold Exceeded - Billing \(4\)”](#) section on page 3-31.

Billing Partition Disk Usage Within Normal Range - Billing (5)

The Billing Partition Disk Usage Within Normal Range event is informational and no further action is required.

File Transfer Protocol/Secure File Transfer Protocol Transfer Failed - Billing (6)

The File Transfer Protocol/Secure File Transfer Protocol Transfer Failed alarm (major) indicates that the billing information FTP/SFTP transfer has failed. To troubleshoot and correct the cause of File Transfer Protocol/Secure File Transfer Protocol Transfer Failed alarm, refer to the [“File Transfer Protocol/Secure File Transfer Protocol Transfer Failed - Billing \(6\)” section on page 3-32](#).

**Note**

OpenSSH version 3.9p1 contains a bug that may cause billing file transfers over SFTP to fail.

Transmission Control Protocol Connection Error - Billing (7)

The Transmission Control Protocol Connection Error alarm (critical) indicates that an error has occurred on the TCP connection. To troubleshoot and correct the cause of the Transmission Control Protocol Connection Error alarm, refer to the [“Transmission Control Protocol Connection Error - Billing \(7\)” section on page 3-33](#).

Transmission Control Protocol Packet Receive Failure - Billing (8)

The Transmission Control Protocol Packet Receive Failure alarm (major) indicates that a TCP packet receive failure has occurred. To troubleshoot and correct the cause of the Transmission Control Protocol Packet Receive Failure alarm, refer to the [“Transmission Control Protocol Packet Receive Failure - Billing \(8\)” section on page 3-33](#).

Database Connection Error - Billing (13)

The Database Connection Error alarm (critical) indicates that a database connection error has occurred. To troubleshoot and correct the cause of the Database Connection Error alarm, refer to the [“Database Connection Error - Billing \(13\)” section on page 3-33](#).

File Open Error - Billing (14)

The File Open Error event serves as a warning that a file open error has occurred. The primary cause of a file open error is a system malfunction. The system may be out of file descriptors. If a file open error has occurred, contact Cisco TAC to obtain technical assistance. Refer to the [“Obtaining Technical Assistance” section on page xxxviii](#) for detailed instructions on contacting Cisco TAC and opening a service request.

File Write Error - Billing (15)

The File Write Error alarm (major) indicates that a file write error has occurred. To troubleshoot and correct the cause of the File Write Error alarm, refer to the [“File Write Error - Billing \(15\)” section on page 3-33](#).

Call Data Block Send Failed - Billing (29)

The Call Data Block Send Failed alarm (major) indicates that a call data block (CDB) send has failed. To troubleshoot and correct the cause of the Call Data Block Send Failed alarm, refer to the [“Call Data Block Send Failed - Billing \(29\)” section on page 3-33](#).

Domain Name Mapping Failed - Billing (30)

The Domain Name Mapping Failed alarm (major) indicates that a domain name mapping has failed. To troubleshoot and correct the cause of the Domain Name Mapping Failed alarm, refer to the [“Domain Name Mapping Failed - Billing \(30\)” section on page 3-34](#).

Port not Specified - Billing (31)

The Port not Specified alarm (major) indicates that a port has not been specified or configured. To troubleshoot and correct the cause of the Port not Specified alarm, refer to the [“Port not Specified - Billing \(31\)” section on page 3-34](#).

Element Management System Address not Specified - Billing (32)

The Element Management System Address not Specified alarm (major) indicates that an EMS address has not been specified or configured. To troubleshoot and correct the cause of the Element Management System Address not Specified alarm, refer to the [“Element Management System Address not Specified - Billing \(32\)” section on page 3-34](#).

File Transfer Protocol/Secure File Transfer Protocol Parameters Invalid - Billing (33)

The File Transfer Protocol/Secure File Transfer Protocol Parameters Invalid alarm (major) indicates that the FTP/SFTP parameters configuration is not valid or has not been fully configured. To troubleshoot and correct the cause of the File Transfer Protocol/Secure File Transfer Protocol Parameters Invalid alarm, refer to the [“File Transfer Protocol/Secure File Transfer Protocol Parameters Invalid - Billing \(33\)” section on page 3-34](#).

All Billing Links at Billing Server Down - Billing (35)

The All Billing Links at Billing Server Down alarm (critical) indicates that all of the billing links to the billing server are down. To troubleshoot and correct the cause of the All Billing Links at Billing Server Down alarm, refer to the [“All Billing Links at Billing Server Down - Billing \(35\)” section on page 3-34](#).

Billing Link Restored - Billing (36)

The Billing Link Restored event is informational and no further action is required. The primary cause of the Billing Link Restored event is that the cable to the billing server or the link to the billing server has been restored.

Billing Link Failure - Billing (37)

The Billing Link Failure alarm (major) indicates that a link to the billing server has failed. To troubleshoot and correct the cause of the Billing Link Failure alarm, refer to the [“Billing Link Failure - Billing \(37\)” section on page 3-35](#).

Event Message Log File Access Error - Billing (38)

The Event Message Log File Access Error alarm (major) indicates that an event message (EM) log file access error has occurred. To troubleshoot and correct the cause of the Event Message Log File Access Error alarm, refer to the [“Event Message Log File Access Error - Billing \(38\)” section on page 3-35](#).

RADIUS Accounting Receive Failure - Billing (39)

The RADIUS Accounting Receive Failure alarm (minor) indicates that a RADIUS accounting receive has failed. To troubleshoot and correct the cause of the RADIUS Accounting Receive Failure alarm, refer to the [“RADIUS Accounting Receive Failure - Billing \(39\)” section on page 3-35](#).

Event Message Encode Failure - Billing (40)

The Event Message Encode Failure alarm (minor) indicates that an EM encode failure has occurred. To troubleshoot and correct the cause of the Event Message Encode Failure alarm, refer to the [“Event Message Encode Failure - Billing \(40\)” section on page 3-35](#).

Message Content Error - Billing (41)

The Message Content Error alarm (minor) indicates that a message content error has occurred. To troubleshoot and correct the cause of the Message Content Error alarm, refer to the [“Message Content Error - Billing \(41\)” section on page 3-35](#).

Error Reading Provisioned Data—Using Default - Billing (42)

The Error Reading Provisioned Data—Using Default event functions as a warning that an error occurred while reading provisioning data and that the default provisioning data and default values will be used. The primary cause of the error is that the application was unable to read provisioned data, and had to resort to using default values. Check to ensure a complete load has been installed on the Cisco BTS 10200 Softswitch system. If the load is complete and problem persists, contact Cisco TAC. Refer to the [“Obtaining Technical Assistance” section on page xxxviii](#) for detailed instructions on contacting Cisco TAC and opening a service request.

Record Keeping System Switch Occurred - Billing (44)

The Record Keeping System Switch Occurred alarm (major) indicates that a RKS switch has occurred. To troubleshoot and correct the cause of the Record Keeping System Switch Occurred alarm, refer to the [“Record Keeping System Switch Occurred - Billing \(44\)” section on page 3-36](#).

Event Message Log File Opened - Billing (45)

The Event Message Log File Opened alarm (minor) indicates that a event message log file has been opened. To troubleshoot and correct the cause of the Event Message Log File Opened alarm, refer to the [“Event Message Log File Opened - Billing \(45\)” section on page 3-36](#).

Event Message Log File Closed - Billing (46)

The Event Message Log File Closed alarm (minor) indicates that a event message log file has been closed. To troubleshoot and correct the cause of the Event Message Log File Closed alarm, refer to the [“Event Message Log File Closed - Billing \(46\)” section on page 3-36](#).

Record Keeping System Unreachable for One Hour - Billing (47)

The Record Keeping System Unreachable for One Hour alarm (minor) indicates that the RKS servers have been unreachable for one hour. To troubleshoot and correct the cause of the Record Keeping System Unreachable for One Hour alarm, refer to the [“Record Keeping System Unreachable for One Hour - Billing \(47\)” section on page 3-36](#).

Record Keeping System Unreachable for Three Hours - Billing (48)

The Record Keeping System Unreachable for Three Hours alarm (major) indicates that the RKS servers have been unreachable for three hours. To troubleshoot and correct the cause of the Record Keeping System Unreachable for Three Hours alarm, refer to the [“Record Keeping System Unreachable for Three Hours - Billing \(48\)” section on page 3-36](#).

Record Keeping System Unreachable for Five Hours - Billing (49)

The Record Keeping System Unreachable for Five Hours alarm (critical) indicates that the RKS servers have been unreachable for five hours. To troubleshoot and correct the cause of the Record Keeping System Unreachable for Five Hours alarm, refer to the [“Record Keeping System Unreachable for 5 Hours - Billing \(49\)” section on page 3-37](#).

Bulk Data Management System Stopped Generating New Billing File - Billing (52)

The Bulk Data Management System Stopped Generating New Billing File alarm (critical) indicates that the BDMS has stopped generating new billing files. To troubleshoot and correct the cause of the Bulk Data Management System Stopped Generating New Billing File alarm, refer to the [“Bulk Data Management System Stopped Generating New Billing File - Billing \(52\)”](#) section on page 3-37.

Event Message Disk Space 50 Percent Full - Billing (53)

The Event Message Disk Space 50 Percent Full alarm (minor) indicates that the event message disk space is 50 percent full. To troubleshoot and correct the cause of the Event Message Disk Space 50 Percent Full alarm, refer to the [“Event Message Disk Space 50 Percent Full - Billing \(53\)”](#) section on page 3-37.

Event Message Disk Space 70 Percent Full - Billing (54)

The Event Message Disk Space 70 Percent Full alarm (major) indicates that the event message disk space is 70 percent full. To troubleshoot and correct the cause of the Event Message Disk Space 70 Percent Full alarm, refer to the [“Event Message Disk Space 70 Percent Full - Billing \(54\)”](#) section on page 3-37.

Event Message Disk Space 100 Percent Full - Billing (55)

The Event Message Disk Space 100 Percent Full alarm (critical) indicates that the event message disk space is 100 percent full. To troubleshoot and correct the cause of the Event Message Disk Space 100 Percent Full alarm, refer to the [“Event Message Disk Space 100 Percent Full - Billing \(55\)”](#) section on page 3-37.

Billing Data Corruption Detected - Billing (56)

The Billing Data Corruption Detected alarm (critical) indicates that a billing data corruption has been detected. To troubleshoot and correct the cause of the Billing Data Corruption Detected alarm, refer to the [“Billing Data Corruption Detected - Billing \(56\)”](#) section on page 3-38.

Prepaid Subscriber Call Attempt Failed Because of Balance - Billing (57)

The Prepaid Subscriber Call Attempt Failed Because of Balance event functions as informational alert that a prepaid subscriber call attempt has failed of the subscriber account balance. The primary cause of the event is that the subscriber has an insufficient balance to place the attempted call. To correct the primary cause of the event, ask the subscriber to deposit more money in their account. Additionally, there may be a problem with the billing information on the prepaid server. To correct the secondary cause of the event, verify the billing information on the prepaid server.

Signaling Prepaid Server Inaccessible - Billing (58)

The Signaling Prepaid Server Inaccessible alarm (major) indicates that the signaling prepaid server has become inaccessible. To troubleshoot and correct the cause of the Signaling Prepaid Server Inaccessible alarm, refer to the [“Signaling Prepaid Server Inaccessible - Billing \(58\)”](#) section on page 3-38.

Troubleshooting Billing Alarms

This section provides the information needed to troubleshoot and correct Billing events. [Table 3-3](#) lists all Billing events in numerical order and provides cross reference to each subsection in this section.

Table 3-3 *Cisco BTS 10200 Softswitch Billing Alarms*

Alarm Type	Alarm Name	Alarm Severity
BILLING(2)	Billing Partition Disk Usage Minor Threshold Exceeded - Billing (2)	MINOR
BILLING(3)	Billing Partition Disk Usage Major Threshold Exceeded - Billing (3)	MAJOR
BILLING(4)	Billing Partition Disk Usage Critical Threshold Exceeded - Billing (4)	CRITICAL
BILLING(6)	File Transfer Protocol/Secure File Transfer Protocol Transfer Failed - Billing (6)	MAJOR
BILLING(7)	Transmission Control Protocol Connection Error - Billing (7)	CRITICAL
BILLING(8)	Transmission Control Protocol Packet Receive Failure - Billing (8)	MAJOR
BILLING(13)	Database Connection Error - Billing (13)	CRITICAL
BILLING(15)	File Write Error - Billing (15)	MAJOR
BILLING(29)	Call Data Block Send Failed - Billing (29)	MAJOR
BILLING(30)	Domain Name Mapping Failed - Billing (30)	MAJOR
BILLING(31)	Port not Specified - Billing (31)	MAJOR
BILLING(32)	Element Management System Address not Specified - Billing (32)	MAJOR
BILLING(33)	File Transfer Protocol/Secure File Transfer Protocol Parameters Invalid - Billing (33)	MAJOR
BILLING(35)	All Billing Links at Billing Server Down - Billing (35)	CRITICAL
BILLING(37)	Billing Link Failure - Billing (37)	MAJOR
BILLING(38)	Event Message Log File Access Error - Billing (38)	MAJOR
BILLING(39)	RADIUS Accounting Receive Failure - Billing (39)	MINOR
BILLING(40)	Event Message Encode Failure - Billing (40)	MINOR
BILLING(41)	Message Content Error - Billing (41)	MINOR
BILLING(44)	Record Keeping System Switch Occurred - Billing (44)	MAJOR
BILLING(45)	Event Message Log File Opened - Billing (45)	MINOR
BILLING(46)	Event Message Log File Closed - Billing (46)	MINOR
BILLING(47)	Record Keeping System Unreachable for One Hour - Billing (47)	MINOR
BILLING(48)	Record Keeping System Unreachable for Three Hours - Billing (48)	MAJOR
BILLING(49)	Record Keeping System Unreachable for 5 Hours - Billing (49)	CRITICAL
BILLING(52)	Bulk Data Management System Stopped Generating New Billing File - Billing (52)	CRITICAL
BILLING(53)	Event Message Disk Space 50 Percent Full - Billing (53)	MINOR
BILLING(54)	Event Message Disk Space 70 Percent Full - Billing (54)	MAJOR
BILLING(55)	Event Message Disk Space 100 Percent Full - Billing (55)	CRITICAL
BILLING(56)	Billing Data Corruption Detected - Billing (56)	CRITICAL
BILLING(58)	Signaling Prepaid Server Inaccessible - Billing (58)	MAJOR

Billing Partition Disk Usage Minor Threshold Exceeded - Billing (2)

The Billing Partition Disk Usage Minor Threshold Exceeded alarm (minor) indicates that a billing partition disk usage minor threshold crossing has occurred. The primary cause of the alarm is that call detail records are accumulating on the disk associated with the billing database in the EMS. This is because data is being written into the database faster than it is being read out of the database. The minor threshold (default value = 70%) has been exceeded. Some fluctuation in disk usage is to be expected as call volume rises and falls during the day. Threshold crossings might step upward (from MINOR to MAJOR to CRITICAL) when there is a rapid increase in call volume, and then step downward (CRITICAL to MAJOR to MINOR) when call volume slows. To correct the primary cause of the alarm, monitor the alarm. The read should catch up to write within a few minutes, and the alarm should not remain active. To monitor the alarm, use the subscribe alarm-report command. To obtain a summary, use the report alarm-summary command. Verify that type=billing is entered in these commands.

Billing Partition Disk Usage Major Threshold Exceeded - Billing (3)

The Billing Partition Disk Usage Major Threshold Exceeded alarm (major) indicates that a billing partition disk usage major threshold crossing has occurred. The primary cause of the alarm is that call detail records are accumulating on the disk associated with the billing database in the EMS. This is because data is being written into the database faster than it is being read out of the database. The major threshold (default value = 80%) has been exceeded. Some fluctuation in disk usage is to be expected as call volume rises and falls during the day. Threshold crossings might step upward (from MINOR to MAJOR to CRITICAL) when there is a rapid increase in call volume, and then step downward (CRITICAL to MAJOR to MINOR) when call volume slows. To correct the primary cause of the alarm, monitor this alarm. The read should catch up to write within a few minutes, and the alarm should not remain active. To monitor the alarm, use the subscribe alarm-report command. To obtain a summary, use the report alarm-summary command. Verify that type=billing is entered in these commands. If the alarm does not clear (or step down to a reduced level) in a few minutes, contact Cisco TAC for assistance. Refer to the [“Obtaining Technical Assistance”](#) section on page xxxviii for detailed instructions on contacting Cisco TAC and opening a service request.

Billing Partition Disk Usage Critical Threshold Exceeded - Billing (4)

The Billing Partition Disk Usage Critical Threshold Exceeded alarm (critical) indicates that a billing partition disk usage critical threshold crossing has occurred. The primary cause of the alarm is that call detail records are accumulating on the disk associated with the billing database in the EMS. This is because data is being written into the database faster than it is being read out of the database. The major threshold (default value = 90%) has been exceeded. Some fluctuation in disk usage is to be expected as call volume rises and falls during the day. Threshold crossings might step upward (from MINOR to MAJOR to CRITICAL) when there is a rapid increase in call volume, and then step downward (CRITICAL to MAJOR to MINOR) when call volume slows. To correct the primary cause of the alarm, Monitor this alarm. The read should catch up to write within a few minutes, and the alarm should not remain active. To monitor the alarm, use the subscribe alarm-report command. To obtain a summary, use the report alarm-summary command. Verify that type=billing is entered in these commands. If the alarm does not clear (or step down to a reduced level) in a few minutes, contact Cisco TAC for assistance. Refer to the [“Obtaining Technical Assistance”](#) section on page xxxviii for detailed instructions on contacting Cisco TAC and opening a service request.

File Transfer Protocol/Secure File Transfer Protocol Transfer Failed - Billing (6)

The File Transfer Protocol/Secure File Transfer Protocol Transfer Failed alarm (major) indicates that the billing information FTP/SFTP transfer has failed. The primary cause of the alarm is that the Cisco BTS 10200 Softswitch is unable to connect to remote host. To correct the primary cause of the alarm, verify the remote host is reachable. Run “show billing-acct-addr” and verify that the billing-server-addr is correct. Change the billing-server-addr, if necessary, via “change billing-acct-addr”. The secondary cause of the alarm is that the Cisco BTS 10200 Softswitch is unable to login to remote host. To correct the secondary cause of the alarm, use the “show billing-acct-addr” to verify that the user-name is a valid user for the host specified in billing-server-addr. If user-name is correct and the “TransferType” dataword shows “FTP”, re-enter the password via “change billing-acct-addr”. If user-name is correct and the “TransferType” dataword shows “SFTP”, verify that SSH keys have been pre-configured for user-name on both the Cisco BTS 10200 Softswitch and the remote host. The tertiary cause of the alarm is that a file transfer error occurred. To correct the tertiary cause of the alarm, check the “Error” dataword to see if it gives an indication of the kind of error that occurred. It could be a file-system error on the remote host, or a communication failure between the Cisco BTS 10200 Softswitch and the remote host. The subsequent cause of the alarm is that the CDB_BILLING_SUPP flag is not set to “Y” in the call-agent-profile table. To correct the subsequent cause of the alarm, check and verify that the CDB_BILLING_SUPP flag is set to “Y” in the call-agent-profile table



Note

OpenSSH version 3.9p1 contains a bug that may cause billing file transfers over SFTP to fail.

Use the following information to check the datawords:

The datawords generated by the alarm are Filename (40), FTP address (40), and error (50), where:

- **file name**—The name of file that the Softswitch is attempting to send to the billing server.
- **FTP address**—The IP address/domain name of the billing server that the Cisco BTS 10200 Softswitch is attempting to reach.
- **error**—One or more of the following data words can be displayed to indicate missing or incorrect information:
 - **Login**—The username for the billing server is missing or incorrect in the database, or the username does not have the privilege level to write to the specified directory on the remote billing server.
 - **Password**—The password for the billing server is missing or incorrect in the database.
 - **Connection**—The billing-server-addr (IP address/domain name of billing server) is missing or incorrect in the database, or the connection to the billing server is unavailable.
 - **Repository**—The billing-server-directory identifier is missing or incorrect in the database, or the specified directory is not available on the billing server.

The alarm indicates a failure in making the FTP connection to the remote billing server to transfer billing information from the EMS. This can happen if:

1. The FTP information has not been initialized.
2. The information in the Softswitch database does not match the remote billing server:
 - a. The login username (for the billing server) is missing or incorrect in the database.
 - b. The username is correct but does not have the privilege level to write to the specified directory.
 - c. The password (for the remote billing server) is missing or incorrect in the database.
 - d. The billing-server-addr (IP address/domain name) is missing or incorrect in the database.

- e. The billing-server-directory identifier (repository) is missing or incorrect in the database.
- 3. The connection to the remote billing server is unavailable.
- 4. The specified directory is not available on the remote billing server.

Transmission Control Protocol Connection Error - Billing (7)

The Transmission Control Protocol Connection Error alarm (critical) indicates that an error has occurred on the TCP connection. The primary cause of the alarm is a system call error. To correct the primary cause of the alarm, check the address of the Billing server in the Cisco BTS 10200 Softswitch platform configuration. The secondary cause of the alarm is the Cisco BTS 10200 Softswitch is not connected to the right address. To correct the secondary cause of the alarm, call Cisco TAC for technical support. Refer to the [“Obtaining Technical Assistance”](#) section on page xxxviii for detailed instructions on contacting Cisco TAC and opening a service request.

Transmission Control Protocol Packet Receive Failure - Billing (8)

The Transmission Control Protocol Packet Receive Failure alarm (major) indicates that a TCP packet receive failure has occurred. The primary cause of the alarm is that the peer went down and the socket closed. To correct the primary cause of the alarm, check the status of the peer and bring it up if it is down.

Database Connection Error - Billing (13)

The Database Connection Error alarm (critical) indicates that a database connection error has occurred. The primary cause of the alarm is that the SQL server is down. To correct the primary cause of the alarm, restart SQL server. If restarting SQL server does not correct the problem and clear the alarm, contact Cisco TAC for technical support. Refer to the [“Obtaining Technical Assistance”](#) section on page xxxviii for detailed instructions on contacting Cisco TAC and opening a service request.

File Write Error - Billing (15)

The File Write Error alarm (major) indicates that a file write error has occurred. The primary cause of the alarm is that a system error has occurred. The Cisco BTS 10200 Softswitch system may be out of file descriptors. To correct the primary cause of the alarm, contact Cisco TAC for technical support. Refer to the [“Obtaining Technical Assistance”](#) section on page xxxviii for detailed instructions on contacting Cisco TAC and opening a service request.

Call Data Block Send Failed - Billing (29)

The Call Data Block Send Failed alarm (major) indicates that a CDB send has failed. The primary cause of the alarm is that a TCP send call has failed. To correct the primary cause of the alarm, check the port number and address of blg and bmg processes in the platform.cfg file. The secondary cause of the alarm is that both the EMS servers are down. To correct the secondary cause of the alarm, check if both EMS servers are down. If both EMS servers are down, bring at least one EMS server up.

Domain Name Mapping Failed - Billing (30)

The Domain Name Mapping Failed alarm (major) indicates that a domain name mapping has failed. The primary cause of the alarm is that the wrong DNS server name mapping is specified in the Cisco BTS 10200 Softswitch configuration files. To correct the primary cause of the alarm, check the `optical.cfg` and `platform.cfg` files for the correct mapping information.

Port not Specified - Billing (31)

The Port not Specified alarm (major) indicates that a port has not been specified or configured. The primary cause of the alarm is that the port is not specified in `platform.cfg` file. To correct the primary cause of the alarm, check the `platform.cfg` file and add the argument to `blg -port 15260`.

Element Management System Address not Specified - Billing (32)

The Element Management System Address not Specified alarm (major) indicates that an EMS address has not been specified or configured. The primary cause of the alarm is that either the primary or secondary EMS address has not been specified in the `platform.cfg` file. To correct the primary cause of the alarm, check the `platform.cfg` file to verify the process `BLG` and to add the missing addresses to the file.

File Transfer Protocol/Secure File Transfer Protocol Parameters Invalid - Billing (33)

The File Transfer Protocol/Secure File Transfer Protocol Parameters Invalid alarm (major) indicates that the FTP/SFTP parameters configuration is not valid or has not been fully configured. The primary cause of the alarm is that the `billing-acct-addr` table is not fully provisioned with the information needed to perform file transfers. To correct the primary cause of the alarm, check `billing-acct-addr` fields via “`show billing-acct-addr`” command. For FTP file transfer, ensure `billing-server-addr`, `billing-server-directory`, `user-name`, and `password` (not displayed) are provisioned. Also ensure `sftp-supp` is set to “N”. For SFTP file transfer, ensure `billing-server-addr`, `billing-server-directory`, and `user-name` are provisioned. Also ensure `sftp-supp` is set to “Y”.

All Billing Links at Billing Server Down - Billing (35)

The All Billing Links at Billing Server Down alarm (critical) indicates that all of the billing links to the billing server are down. The primary cause of the alarm is that the cable connection to the Billing Server may have been pulled out. To correct the primary cause of the alarm, restore cable connection to the Billing Server. The secondary cause of the alarm is that an “`ifconfig down`” command may have been executed on the interfaces. To correct the secondary cause of the alarm, execute an “`ifconfig up`” command on the interfaces.

Billing Link Failure - Billing (37)

The Billing Link Failure alarm (major) indicates that a link to the billing server has failed. The primary cause of the alarm is that an interface cable may have been pulled. To correct the primary cause of the alarm, restore cable connection. The secondary cause of the alarm is that an “ifconfig down” command may have been executed on the interface. To correct the secondary cause of the alarm, execute and “ifconfig up” command on the interface.

Event Message Log File Access Error - Billing (38)

The Event Message Log File Access Error alarm (major) indicates that an EM log file access error has occurred. The primary cause of the alarm is that a system error has occurred. The Cisco BTS 10200 Softswitch system may be out of file descriptors. To correct primary cause of the alarm, contact Cisco TAC. Refer to the [“Obtaining Technical Assistance” section on page xxxviii](#) for detailed instructions on contacting Cisco TAC and opening a service request. The secondary cause of the alarm is that a system hard drive may be faulty. To verify the secondary cause of the alarm, cause the BDMS to switch over to its mate node.

RADIUS Accounting Receive Failure - Billing (39)

The RADIUS Accounting Receive Failure alarm (minor) indicates that a RADIUS accounting receive has failed. The primary cause of the alarm is that a system error has occurred. If the problem persists, contact Cisco TAC. Refer to the [“Obtaining Technical Assistance” section on page xxxviii](#) for detailed instructions on contacting Cisco TAC and opening a service request.

Event Message Encode Failure - Billing (40)

The Event Message Encode Failure alarm (minor) indicates that an EM encode failure has occurred. The primary cause of the alarm is that there is a problem with the format of the data being sent to the RKS. To correct the primary cause of the alarm, contact Cisco TAC. Refer to the [“Obtaining Technical Assistance” section on page xxxviii](#) for detailed instructions on contacting Cisco TAC and opening a service request.

Message Content Error - Billing (41)

The Message Content Error alarm (minor) indicates that a message content error has occurred. The primary cause of the alarm is that there is a mismatch between what the sender populated in the message and what the receiver expects. To correct the primary cause of the alarm, contact Cisco TAC. Refer to the [“Obtaining Technical Assistance” section on page xxxviii](#) for detailed instructions on contacting Cisco TAC and opening a service request.

Record Keeping System Switch Occurred - Billing (44)

The Record Keeping System Switch Occurred alarm (major) indicates that a RKS switch has occurred. The primary cause of the alarm is that billing changed the destination RKS for transmitting event messages. The change could have been triggered by a communication problem with an RKS, or by an attempt to reestablish RKS communication. No further action is required to correct the primary cause of the alarm.

Event Message Log File Opened - Billing (45)

The Event Message Log File Opened alarm (minor) indicates that a event message log file has been opened. The primary cause of the alarm is that a log file has been created for the storage of event messages that cannot be transmitted to an RKS. No further action is required to correct the primary cause of the alarm.

Event Message Log File Closed - Billing (46)

The Event Message Log File Closed alarm (minor) indicates that a event message log file has been closed. The primary cause of the alarm is that an open event message log file has been closed. No further action is required to correct the primary cause of the alarm.

Record Keeping System Unreachable for One Hour - Billing (47)

The Record Keeping System Unreachable for One Hour alarm (minor) indicates that the RKS servers have been unreachable for one hour. The primary cause of the alarm is that billing has not been able to communicate with any RKS for the past one hour. To correct the primary cause of the alarm, check the status of the primary and secondary RKS servers and attempt to bring them into service. Verify that the radius-profile table and call-agent-profile table are provisioned such that communication with the RKS servers is possible.

Record Keeping System Unreachable for Three Hours - Billing (48)

The Record Keeping System Unreachable for Three Hours alarm (major) indicates that the RKS servers have been unreachable for three hours. The primary cause of the alarm is that billing has not been able to communicate with any RKS for the past three hours. To correct the primary cause of the alarm, check the status of the primary and secondary RKS servers and attempt to bring them into service. Verify that the radius-profile table and call-agent-profile table are provisioned such that communication with the RKS servers is possible.

Record Keeping System Unreachable for 5 Hours - Billing (49)

The Record Keeping System Unreachable for 5 Hours alarm (critical) indicates that the RKS servers have been unreachable for five hours. The primary cause of the alarm is that billing has not been able to communicate with any RKS for the past five hours. To correct the primary cause of the alarm, check the status of the primary and secondary RKS servers and attempt to bring them into service. Verify that the radius-profile table and call-agent-profile table are provisioned such that communication with the RKS servers is possible.

Bulk Data Management System Stopped Generating New Billing File - Billing (52)

The Bulk Data Management System Stopped Generating New Billing File alarm (critical) indicates that the BDMS has stopped generating new billing files. The primary cause of the alarm is that call detail records are accumulating on the disk associated with the billing files in the EMS. This is because data is being written into the billing files faster than it is being forwarded to the Billing Mediation Server. FTP to the Billing Mediation Server may not be working. The maximum disk partition for billing has been exceeded or the maximum number of files has been exceeded. To correct the primary cause of the alarm, check the Billing Mediation Server node name, user name and password specified in BILLING_ACCT_ADDR table and log files. Correct any errors to let FTP start again. If `billing_server_directory = "/dev/null"`, primary files under `billing_directory` will not be forwarded or deleted automatically. In this case, files have to be manually deleted or moved out, and BDMS needs to be restarted before it will start generating new billing files.

Event Message Disk Space 50 Percent Full - Billing (53)

The Event Message Disk Space 50 Percent Full alarm (minor) indicates that the event message disk space is 50 percent full. The primary cause of the alarm is that the event message storage has reached 50% of the maximum storage space allowed. To correct the primary cause of the alarm, move the event message files out of the specified directory. Store them in another location, or discard them.

Event Message Disk Space 70 Percent Full - Billing (54)

The Event Message Disk Space 70 Percent Full alarm (major) indicates that the event message disk space is 70 percent full. The primary cause of the alarm is that the event message storage has reached 70% of the maximum storage space allowed. To correct the primary cause of the alarm, move the event message files out of the specified directory. Store them in another location, or discard them.

Event Message Disk Space 100 Percent Full - Billing (55)

The Event Message Disk Space 100 Percent Full alarm (critical) indicates that the event message disk space is 100 percent full. The primary cause of the alarm is that the event message storage has been completely filled. No additional event messages will be written to the disk until more space is made available. To correct the primary cause of the alarm, move the event message files out of the specified directory. Store them in another location, or discard them.

Billing Data Corruption Detected - Billing (56)

The Billing Data Corruption Detected alarm (critical) indicates that a billing data corruption has been detected. The primary cause of the alarm is that the billing data stored on disk may have become corrupted due to a power outage, ungraceful shutdown, or hard-drive failure. To correct the primary cause of the alarm, make sure that the BDMS that detected the problem has gone to the out-of-service state. Leave the BDMS in the out-of-service state and contact Cisco TAC for assistance. Refer to the [“Obtaining Technical Assistance” section on page xxxviii](#) for detailed instructions on contacting Cisco TAC and opening a service request.

Signaling Prepaid Server Inaccessible - Billing (58)

The Signaling Prepaid Server Inaccessible alarm (major) indicates that the signaling prepaid server has become inaccessible. The primary cause of the alarm is that all the prepaid servers are down. To correct the primary cause of the alarm, check the operating status of the prepaid servers. If possible, place the prepaid servers back into service. The secondary cause of the alarm is that the IP network between the Cisco BTS 10200 Softswitch POTS FS and the prepaid servers is down. To correct the secondary cause of the alarm, check and correct any problems in IP network.



CHAPTER 4

Call Processing Troubleshooting

Revised: October 23, 2008, OL-11335-06

Introduction

This chapter provides the information needed to monitor and troubleshoot Call Processing events and alarms. This chapter is divided into the following sections:

- [Call Processing Events and Alarms](#) – Provides a brief overview of each Call Processing event and alarm.
- [Monitoring Call Processing Events](#) – Provides the information needed to monitor and correct Call Processing events.
- [Troubleshooting Call Processing Alarms](#) – Provides the information needed to troubleshoot and correct Call Processing alarms.

For additional call processing routing and translations information refer to the *Cisco BTS 10200 Softswitch Routing, Translations, and Dial Plan Guide*.



Note

The following billing records are created when a call is rejected due to overload conditions:

- SS7 termination cause code 42
 - Cable signaling stop event cause code “resource unavailable”
- Calls rejected by the signaling adapter will not generate a billing record.

Call Processing Events and Alarms

This section provides a brief overview of the Call Processing events and alarms for the Cisco BTS 10200 Softswitch in numerical order. [Table 4-1](#) lists all Call Processing events and alarms by severity.


Note

Click the Call Processing message number in [Table 4-1](#) to display information about the event.

Table 4-1 *Call Processing Events and Alarms by Severity*

CRITICAL	MAJOR	MINOR	WARNING	INFO
CALLP (12)		CALLP (11)	CALLP (8)	CALLP (1)
		CALLP (38)	CALLP (16)	CALLP (9)
			CALLP (17)	CALLP (13)
			CALLP (18)	CALLP (14)
			CALLP (19)	CALLP (15)
			CALLP (20)	
			CALLP (21)	
			CALLP (22)	
			CALLP (23)	
			CALLP (24)	
			CALLP (25)	
			CALLP (26)	
			CALLP (27)	
			CALLP (28)	
			CALLP (29)	
			CALLP (30)	
			CALLP (31)	
			CALLP (32)	
			CALLP (33)	
			CALLP (34)	
			CALLP (35)	
			CALLP (36)	
			CALLP (37)	
			CALLP (39)	

CALLP (1)

For additional information, refer to the [“Test Report - Call Processing \(1\)”](#) section on page 4-20.

DESCRIPTION	Test Report
SEVERITY	Information (INFO)
THRESHOLD	10000
THROTTLE	0


Note

CALLP (2) through CALLP (7) are not used.

CALLP (8)

To monitor and correct the cause of the event, refer to the [“No Route Available for Called Number - Call Processing \(8\)”](#) section on page 4-20.

DESCRIPTION	No Route Available for Called Number
SEVERITY	WARNING
THRESHOLD	100
THROTTLE	500
DATAWORDS	Orig Type (Trunk or S - ONE_BYTE Orig Sub or TG ID - EIGHT_BYTES Calling Party Number - STRING [20] Called Party Number - STRING [20]
PRIMARY CAUSE	Call originates from a subscriber or trunk for a called party number that has no route available.
PRIMARY ACTION	The data words in the event report indicate what parameters that need to be corrected. Refer to office records for the subscriber.
SECONDARY CAUSE	Parameter(s) in the subscriber and/or dial-plan table are missing or incorrect for this dialed number.
SECONDARY ACTION	Determine whether the routing parameters (such as digit-string) were entered correctly in the subscriber and dial-plan tables.
TERNARY ACTION	If the called party is a subscriber, verify that the subscriber-type is listed as “subscriber” in the dial-plan table.
SUBSEQUENT ACTION	If the call is long distance using a presubscribed interexchange carrier (PIC), check that the PIC for this subscriber is properly provisioned in the dial-plan table. If necessary, edit these files using the “change dial-plan” or “change subscriber” commands.

CALLP (9)

For additional information, refer to the [“No Route Available for Carrier Dialed - Call Processing \(9\)” section on page 4-20.](#)

DESCRIPTION	No Route Available for Carrier Dialed
SEVERITY	INFO
THRESHOLD	100
THROTTLE	0
DATAWORDS	Orig Type (Trunk or S - ONE_BYTE Orig Sub or TG ID - EIGHT_BYTES Calling Party Number - STRING [20] Called Party Number - STRING [20] Carrier Code Dialed - STRING [20]
PRIMARY CAUSE	No route is available for the interexchange carrier (IXC) dialed.
PRIMARY ACTION	The data words in the event report indicate the parameters that need to be corrected. Refer to office records for the carrier.
SECONDARY CAUSE	Parameter(s) in the carrier and/or route-grp table are missing or incorrect for the carrier.
SECONDARY ACTION	Determine whether the routing parameters were entered correctly in the carrier and/or route-grp tables.
TERNARY ACTION	If the carrier-identification (ID) or route-grp-ID are not specified, or are incorrect, in the dial-plan table, enter the correct values. Use the change carrier or change route-grp command.



Note

CALLP (10) is not used.

CALLP (11)

To troubleshoot and correct the cause of the alarm, refer to the [“Feature Server One Link Down - Call Processing \(11\)” section on page 4-26.](#)

DESCRIPTION	Feature Server One Link Down
SEVERITY	MINOR
THRESHOLD	100
THROTTLE	0
DATAWORDS	Interface Name - STRING [65] Interface IP Address - STRING [65]
PRIMARY CAUSE	Hardware is broken.
PRIMARY ACTION	Check the link interfaces.

CALLP (12)

To troubleshoot and correct the cause of the alarm, refer to the [“Feature Server Both Links Down - Call Processing \(12\)” section on page 4-28](#).

DESCRIPTION	Feature Server Both Links Down
SEVERITY	CRITICAL
THRESHOLD	100
THROTTLE	0
DATAWORDS	Interface Name - STRING [65] Interface IP Address - STRING [65] Interface Name - STRING [65] Interface IP Address - STRING [65]
PRIMARY CAUSE	Hardware is broken.
PRIMARY ACTION	Check the link interfaces.

CALLP (13)

For additional information, refer to the [“Network Access Server Create Connection Error - Call Processing \(13\)” section on page 4-21](#).

DESCRIPTION	Network Access Server Create Connection Error (NAS CRCX Error)
SEVERITY	INFO
THRESHOLD	100
THROTTLE	0
PRIMARY CAUSE	Pre-authentication failure.
PRIMARY ACTION	None

CALLP (14)

For additional information, refer to the [“Network Access Server Authentication Failure - Call Processing \(14\)” section on page 4-21.](#)

DESCRIPTION	Network Access Server Authentication Failure (NAS Authentication Failure)
SEVERITY	INFO
THRESHOLD	100
THROTTLE	0
PRIMARY CAUSE	The authentication, authorization, and accounting (AAA) server denied the request.
PRIMARY ACTION	Check the calling and called numbers.

CALLP (15)

For additional information, refer to the [“Cable Modem Termination System Easily Recognizable Identification Not Found in Media Gateway Table - Call Processing \(15\)” section on page 4-21.](#)

DESCRIPTION	Cable Modem Termination System Easily Recognizable Identification Not Found in Media Gateway Table (CMTS ER ID Not Found in MGW Table)
SEVERITY	INFO
THRESHOLD	100
THROTTLE	0
DATAWORDS	MGW-NAME - STRING [80]
PRIMARY CAUSE	Cable modem termination system (CMTS)/easily recognizable (ER) entry not found in the Media Gateway Table.
PRIMARY ACTION	Provision the CMTS-ER index in the Media Gateway Table.

CALLP (16)

To monitor and correct the cause of the event, refer to the [“Route Index has No Trunk Group Assigned - Call Processing \(16\)”](#) section on page 4-21.

DESCRIPTION	Route Index has No Trunk Group Assigned.
SEVERITY	WARNING
THRESHOLD	100
THROTTLE	0
DATAWORDS	Route Index - FOUR_BYTES
PRIMARY CAUSE	A trunk group was not assigned to the given route.
PRIMARY ACTION	Provision a trunk group for the associated route index.

CALLP (17)

To monitor and correct the cause of the event, refer to the [“Invalid Route Index Used - Call Processing \(17\)”](#) section on page 4-21.

DESCRIPTION	Invalid Route Index Used
SEVERITY	WARNING
THRESHOLD	100
THROTTLE	0
DATAWORDS	Route Index - FOUR_BYTES
PRIMARY CAUSE	An invalid route index was used.
PRIMARY ACTION	Correct the provisioning and assign a valid route index.

CALLP (18)

To monitor and correct the cause of the event, refer to the [“Unable to Play Announcement - Call Processing \(18\)” section on page 4-22](#).

DESCRIPTION	Unable to Play Announcement
SEVERITY	WARNING
THRESHOLD	100
THROTTLE	0
DATAWORDS	Announcement Index - FOUR_BYTES
PRIMARY CAUSE	Announcement was not provisioned correctly.
PRIMARY ACTION	Provision announcement.

CALLP (19)

To monitor and correct the cause of the event, refer to the [“Call Routed to Unprovisioned Subscriber - Call Processing \(19\)” section on page 4-22](#).

DESCRIPTION	Call Routed to Unprovisioned Subscriber
SEVERITY	WARNING
THRESHOLD	100
THROTTLE	0
DATAWORDS	Subscriber Index - FOUR_BYTES Directory Number Dia - STRING [20]
PRIMARY CAUSE	Subscriber was not provisioned correctly.
PRIMARY ACTION	Provision a subscriber.

CALLP (20)

To monitor and correct the cause of the event, refer to the [“No Route or Trunk Group Available to Route Call - Call Processing \(20\)” section on page 4-22.](#)

DESCRIPTION	No Route or Trunk Group Available to Route Call
SEVERITY	WARNING
THRESHOLD	100
THROTTLE	0
DATAWORDS	Calling Number - STRING [20] Called Number - STRING [20] Route Index - FOUR_BYTES Trunk Group ID - FOUR_BYTES
PRIMARY CAUSE	Trunk Group was not provisioned correctly in route.
PRIMARY ACTION	Verify route and trunk group provisioning.

CALLP (21)

To monitor and correct the cause of the event, refer to the [“Call Released Due to Maximum Hop Counts Exceeded - Call Processing \(21\)” section on page 4-22.](#)

DESCRIPTION	Call Released Due to Maximum Hop Counts Exceeded
SEVERITY	WARNING
THRESHOLD	100
THROTTLE	0
DATAWORDS	Calling Number - STRING [20] Called Number - STRING [20] Hop Count - FOUR_BYTES
PRIMARY CAUSE	Hops between destinations is excessive.
PRIMARY ACTION	Reduce number of hops between destinations.

CALLP (22)

To monitor and correct the cause of the event, refer to the [“Trunk Group Index Read Failure - Call Processing \(22\)”](#) section on page 4-22.

DESCRIPTION	Trunk Group Index Read Failure
SEVERITY	WARNING
THRESHOLD	100
THROTTLE	0
DATAWORDS	Trunk Group Index - FOUR_BYTES Call Index - FOUR_BYTES
PRIMARY CAUSE	Trunk Group Index could not be retrieved from call data.
PRIMARY ACTION	Check provisioning.

CALLP (23)

To monitor and correct the cause of the event, refer to the [“Routing Error: Termination is Not a Subscriber - Call Processing \(23\)”](#) section on page 4-22.

DESCRIPTION	Routing Error: Termination is Not a Subscriber
SEVERITY	WARNING
THRESHOLD	100
THROTTLE	0
DATAWORDS	Termination Index - FOUR_BYTES Termination Type - FOUR_BYTES
PRIMARY CAUSE	Destination termination is not provisioned as a subscriber.
PRIMARY ACTION	Check provisioning.

CALLP (24)

To monitor and correct the cause of the event, refer to the [“Invalid Route for Subscriber Index - Call Processing \(24\)” section on page 4-23](#).

DESCRIPTION	Invalid Route for Subscriber Index
SEVERITY	WARNING
THRESHOLD	100
THROTTLE	0
DATAWORDS	Route - STRING [20] Subscriber Index - FOUR_BYTES
PRIMARY CAUSE	Route is not provisioned correctly for specified subscriber.
PRIMARY ACTION	Check provisioning.

CALLP (25)

To monitor and correct the cause of the event, refer to the [“Invalid Route Group for Subscriber Routing - Call Processing \(25\)” section on page 4-23](#).

DESCRIPTION	Invalid Route Group for Subscriber Routing
SEVERITY	WARNING
THRESHOLD	100
THROTTLE	0
DATAWORDS	Route - STRING [20] Subscriber Index - FOUR_BYTES
PRIMARY CAUSE	Route group is not provisioned correctly for specified subscriber.
PRIMARY ACTION	Check provisioning.

CALLP (26)

To monitor and correct the cause of the event, refer to the [“Invalid Trunk Group for Subscriber Routing - Call Processing \(26\)” section on page 4-23](#).

DESCRIPTION	Invalid Trunk Group for Subscriber Routing
SEVERITY	WARNING
THRESHOLD	100
THROTTLE	0
DATAWORDS	Trunk Group Index - FOUR_BYTES Subscriber Index - FOUR_BYTES
PRIMARY CAUSE	Trunk group is not provisioned correctly for specified subscriber.
PRIMARY ACTION	Check provisioning.

CALLP (27)

To monitor and correct the cause of the event, refer to the [“Unable to Route: Blocked by Destination Subscriber Status - Call Processing \(27\)” section on page 4-23](#).

DESCRIPTION	Unable to Route: Blocked by Destination Subscriber Status
SEVERITY	WARNING
THRESHOLD	100
THROTTLE	0
DATAWORDS	Subscriber Index - FOUR_BYTES Subscriber Status - STRING [20]
PRIMARY CAUSE	Subscriber is not in the correct state.
PRIMARY ACTION	Check provisioning.

CALLP (28)

To monitor and correct the cause of the event, refer to the [“Route Name Does Not Exist - Call Processing \(28\)” section on page 4-23](#).

DESCRIPTION	Route Name Does Not Exist
SEVERITY	WARNING
THRESHOLD	100
THROTTLE	0
DATAWORDS	Route Name - STRING [40]
PRIMARY CAUSE	Route is not correctly provisioned.
PRIMARY ACTION	Check provisioning.

CALLP (29)

To monitor and correct the cause of the event, refer to the [“Routing Selection Failure - Call Processing \(29\)” section on page 4-23](#).

DESCRIPTION	Routing Selection Failure
SEVERITY	WARNING
THRESHOLD	100
THROTTLE	0
DATAWORDS	Route Index - FOUR_BYTES Calling Number - STRING [20] Called Number - STRING [20]
PRIMARY CAUSE	Route is not correctly provisioned.
PRIMARY ACTION	Check provisioning.

CALLP (30)

To monitor and correct the cause of the event, refer to the [“Customer-Originated Trace Test Failed - Call Processing \(30\)” section on page 4-24](#).

DESCRIPTION	Customer-Originated Trace Test Failed (COT Test Failed)
SEVERITY	WARNING
THRESHOLD	100
THROTTLE	0
DATAWORDS	Termination Index - FOUR_BYTES
PRIMARY CAUSE	Customer-originated trace (COT) test has failed.
PRIMARY ACTION	Contact Cisco for information on how to debug the problem further. (Contact Cisco Technical Assistance Center (TAC).)

Refer to the [“Obtaining Technical Assistance” section on page xxxviii](#) for detailed instructions on contacting Cisco TAC and opening a service request.

CALLP (31)

To monitor and correct the cause of the event, refer to the [“Call Authorization Failure - Call Processing \(31\)” section on page 4-24](#).

DESCRIPTION	Call Authorization Failure
SEVERITY	WARNING
THRESHOLD	100
THROTTLE	0
DATAWORDS	Calling Number - STRING [20] Called Number - STRING [20]
PRIMARY CAUSE	Due to provisioning the call cannot be completed.
PRIMARY ACTION	Contact Cisco for more information. (Contact Cisco TAC.)

Refer to the [“Obtaining Technical Assistance” section on page xxxviii](#) for detailed instructions on contacting Cisco TAC and opening a service request.

CALLP (32)

To monitor and correct the cause of the event, refer to the [“Country Code Dialing Plan Error - Call Processing \(32\)” section on page 4-24](#).

DESCRIPTION	Country Code Dialing Plan Error
SEVERITY	WARNING
THRESHOLD	100
THROTTLE	0
DATAWORDS	Called Number - STRING [20] Dial Plan Index - FOUR_BYTES
PRIMARY CAUSE	The country code was not found in the dial plan.
PRIMARY ACTION	Check provisioning.

CALLP (33)

To monitor and correct the cause of the event, refer to the [“Invalid Call - Call Processing \(33\)” section on page 4-24](#).

DESCRIPTION	Invalid Call
SEVERITY	WARNING
THRESHOLD	100
THROTTLE	0
DATAWORDS	Calling Number - STRING [20] Called Number - STRING [20]
PRIMARY CAUSE	The call could not be completed because the number entered was invalid.
PRIMARY ACTION	Check provisioning and number dialed.

CALLP (34)

To monitor and correct the cause of the event, refer to the [“Dial Plan Information Not Found for Digits Received - Call Processing \(34\)”](#) section on page 4-24.

DESCRIPTION	Dial Plan Information Not Found for Digits Received
SEVERITY	WARNING
THRESHOLD	100
THROTTLE	0
DATAWORDS	Calling Number - STRING [20] Called Number - STRING [20] Dial Plan Index - FOUR_BYTES
PRIMARY CAUSE	The call could not be completed because the number entered could not be located in the dial-plan.
PRIMARY ACTION	Check provisioning and number dialed.

CALLP (35)

To monitor and correct the cause of the event, refer to the [“Dial Plan Information for Test Call Not Found - Call Processing \(35\)”](#) section on page 4-24.

DESCRIPTION	Dial Plan Information for Test Call Not Found
SEVERITY	WARNING
THRESHOLD	100
THROTTLE	0
DATAWORDS	Dial Plan Index - FOUR_BYTES
PRIMARY CAUSE	The test call could not be completed because the number entered could not be located in the dial-plan.
PRIMARY ACTION	Check provisioning and number tested.

CALLP (36)

To monitor and correct the cause of the event, refer to the [“Invalid or Unknown Nature of Address - Call Processing \(36\)” section on page 4-25](#).

DESCRIPTION	Invalid or Unknown Nature of Address (Invalid or Unknown NOA)
SEVERITY	WARNING
THRESHOLD	100
THROTTLE	0
DATAWORDS	NOA Received - FOUR_BYTES Calling Number - STRING [20] Called Number - STRING [20]
PRIMARY CAUSE	The nature of address (NOA) was incorrect in the dial-plan.
PRIMARY ACTION	Check provisioning.

CALLP (37)

To monitor and correct the cause of the event, refer to the [“Call Failure - Call Processing \(37\)” section on page 4-25](#).

DESCRIPTION	Call Failure
SEVERITY	WARNING
THRESHOLD	100
THROTTLE	0
DATAWORDS	Type of Call - FOUR_BYTES Calling Number - STRING [20] Called Number - STRING [20] Failure Indication - STRING [40]
PRIMARY CAUSE	The call failed for the listed indication.
PRIMARY ACTION	Call Cisco for more information. (Contact Cisco TAC.)

Refer to the [“Obtaining Technical Assistance” section on page xxxviii](#) for detailed instructions on contacting Cisco TAC and opening a service request.

CALLP (38)

To troubleshoot and correct the cause of the alarm, refer to the [“Release Cause 25 Exchange Routing Error Received - Call Processing \(38\)”](#) section on page 4-29.

DESCRIPTION	Release Cause 25 Exchange Routing Error Received
SEVERITY	MINOR
THRESHOLD	100
THROTTLE	0
DATAWORDS	CIC - FOUR_BYTES TGN-ID - FOUR_BYTES DPC - STRING [64] OPC - STRING [64]
PRIMARY CAUSE	Received release (REL) with cause number 25.
PRIMARY ACTION	Log and map the cause to number 31.

CALLP (39)

To monitor and correct the cause of the event, refer to the [“Test Call Blocked Due to Congestion or Isolation - Call Processing \(39\)”](#) section on page 4-25.

DESCRIPTION	Test Call Blocked Due to Congestion or Isolation
SEVERITY	WARNING
THRESHOLD	100
THROTTLE	0
DATAWORDS	CIC- TWO_BYTES TGN-ID - EIGHT_BYTES DPC - STRING [20] OPC - STRING [20]
PRIMARY CAUSE	Initial address message (IAM) for test call blocked due to congestion/isolation.
PRIMARY ACTION	Correct congestion/isolation problem and place test call again from remote system.

Monitoring Call Processing Events

This section provides the information needed to monitor and correct Calling Processing events.

Table 4-2 lists all Calling Processing events in numerical order and provides cross reference to each subsection in this section.

Table 4-2 Cisco BTS 10200 Softswitch Call Processing Events

Event Type	Event Name	Event Severity
CALLP(1)	Test Report - Call Processing (1)	INFO
CALLP(8)	No Route Available for Called Number - Call Processing (8)	WARNING
CALLP(9)	No Route Available for Carrier Dialed - Call Processing (9)	INFO
CALLP(11)	Feature Server One Link Down - Call Processing (11)	MINOR
CALLP(12)	Feature Server Both Links Down - Call Processing (12)	CRITICAL
CALLP(13)	Network Access Server Create Connection Error - Call Processing (13)	INFO
CALLP(14)	Network Access Server Authentication Failure - Call Processing (14)	INFO
CALLP(15)	Cable Modem Termination System Easily Recognizable Identification Not Found in Media Gateway Table - Call Processing (15)	INFO
CALLP(16)	Route Index has No Trunk Group Assigned - Call Processing (16)	WARNING
CALLP(17)	Invalid Route Index Used - Call Processing (17)	WARNING
CALLP(18)	Unable to Play Announcement - Call Processing (18)	WARNING
CALLP(19)	Call Routed to Unprovisioned Subscriber - Call Processing (19)	WARNING
CALLP(20)	No Route or Trunk Group Available to Route Call - Call Processing (20)	WARNING
CALLP(21)	Call Released Due to Maximum Hop Counts Exceeded - Call Processing (21)	WARNING
CALLP(22)	Trunk Group Index Read Failure - Call Processing (22)	WARNING
CALLP(23)	Routing Error: Termination is Not a Subscriber - Call Processing (23)	WARNING
CALLP(24)	Invalid Route for Subscriber Index - Call Processing (24)	WARNING
CALLP(25)	Invalid Route Group for Subscriber Routing - Call Processing (25)	WARNING
CALLP(26)	Invalid Trunk Group for Subscriber Routing - Call Processing (26)	WARNING
CALLP(27)	Unable to Route: Blocked by Destination Subscriber Status - Call Processing (27)	WARNING
CALLP(28)	Route Name Does Not Exist - Call Processing (28)	WARNING
CALLP(29)	Routing Selection Failure - Call Processing (29)	WARNING
CALLP(30)	Customer-Originated Trace Test Failed - Call Processing (30)	WARNING
CALLP(31)	Call Authorization Failure - Call Processing (31)	WARNING
CALLP(32)	Country Code Dialing Plan Error - Call Processing (32)	WARNING
CALLP(33)	Invalid Call - Call Processing (33)	WARNING
CALLP(34)	Dial Plan Information Not Found for Digits Received - Call Processing (34)	WARNING
CALLP(35)	Dial Plan Information for Test Call Not Found - Call Processing (35)	WARNING
CALLP(36)	Invalid or Unknown Nature of Address - Call Processing (36)	WARNING
CALLP(37)	Call Failure - Call Processing (37)	WARNING

Table 4-2 Cisco BTS 10200 Softswitch Call Processing Events (continued)

Event Type	Event Name	Event Severity
CALLP(38)	Release Cause 25 Exchange Routing Error Received - Call Processing (38)	MINOR
CALLP(39)	Test Call Blocked Due to Congestion or Isolation - Call Processing (39)	WARNING

Test Report - Call Processing (1)

The Test Report event is used for testing the call processing event category. The event is informational and no further action is required.

No Route Available for Called Number - Call Processing (8)

The No Route Available for Called Number event functions as a warning that there is no route available for the number called. The primary cause for the event is that the call originates from a subscriber or trunk for a called party number that has no route available. The Orig Type (one byte), Orig Sub or trunk group (TG) ID (eight bytes), calling party number (20), and called party number (20) data words in the event report indicate what parameters that need to be corrected. Refer to office records for the subscriber. The secondary cause for the event is that parameters in the subscriber and/or dial-plan table are missing or incorrect for the number dialed. To correct any parameter error, determine whether the routing parameters (such as digit-string) were entered incorrectly in the subscriber and dial-plan tables. If the called party is a subscriber, verify that the subscriber-type is listed as a 'subscriber' in the dial-plan table. If the call is long distance using a PIC, check that the PIC for this subscriber is properly provisioned in the dial-plan table. If necessary, edit these files using the **change dial-plan** or **change subscriber** commands.

No Route Available for Carrier Dialed - Call Processing (9)

The No Route Available for Carrier Dialed event functions as a warning that is no route available for the dialed carrier. The primary cause for the event is that no route is available for the IXC dialed. The Orig Type (one byte), Orig Sub or TG ID (eight bytes), calling party number (20), called party number (20), and carrier code dialed (20) data words in the event report indicate the parameters that need to be corrected. Refer to office records for the carrier. The secondary cause for the event is that parameters in the carrier and/or route-grp table are missing or incorrect for the carrier. Determine whether the routing parameters were entered correctly in the carrier and/or route-grp tables. If the Carrier-ID or Route-Grp-ID are not specified, or are incorrect, in the dial-plan table, enter the correct values. Use the **change carrier** or **change route-grp** command.

Feature Server One Link Down - Call Processing (11)

The Feature Server One Link Down alarm (minor) indicates that one link to the feature server is down. To troubleshoot and correct the cause of the Feature Server One Link Down alarm, refer to the [“Feature Server One Link Down - Call Processing \(11\)”](#) section on page 4-26.

Feature Server Both Links Down - Call Processing (12)

The Feature Server Both Links Down alarm (critical) indicates that both links to the feature server are down. To troubleshoot and correct the cause of the Feature Server Both Links Down alarm, refer to the [“Feature Server Both Links Down - Call Processing \(12\)”](#) section on page 4-28.

Network Access Server Create Connection Error - Call Processing (13)

The Network Access Server Create Connection Error event functions as an informational alert that a network access server (NAS) create connection (CRCX) pre-authentication has failed. The event is informational and no further action is required.

Network Access Server Authentication Failure - Call Processing (14)

The Network Access Server Authentication Failure event functions as an informational alert that a NAS authentication failure has occurred. The primary cause of the event is the AAA server denied the request. Check the calling and called numbers.

Cable Modem Termination System Easily Recognizable Identification Not Found in Media Gateway Table - Call Processing (15)

The Cable Modem Termination System Easily Recognizable Identification Not Found in Media Gateway Table event functions as an informational alert that the CMTS ER ID was not found in the media gateway (MGW) table. The primary cause of the event is that the CMTS/ER entry was not found in the media gateway table. To correct the cause of the event, provision the CMTS-ER index in the media gateway table.

Route Index has No Trunk Group Assigned - Call Processing (16)

The Route Index has No Trunk Group Assigned event functions as a warning that the route index has no trunk group assigned. The primary cause of the event is that a trunk group was not assigned to the given route. To correct the cause of the event, provision a trunk group for the associated route index.

Invalid Route Index Used - Call Processing (17)

The Invalid Route Index Used event functions as a warning that an invalid route index is being used. The primary cause of the event is that an invalid route index is being used. To correct the cause of the event, correct the Cisco BTS 10200 Softswitch provisioning by assigning a valid route index.

Unable to Play Announcement - Call Processing (18)

The Unable to Play Announcement event functions as a warning that an announcement was not played. The primary cause of the event is that the announcement was not provisioned correctly. To correct the primary cause of the event, check the provisioning of the announcement and verify that the announcement is provisioned correctly.

Call Routed to Unprovisioned Subscriber - Call Processing (19)

The Call Routed to Unprovisioned Subscriber event functions as a warning that a call was routed to an unprovisioned subscriber. The primary cause of the event is that the subscriber account was not properly provisioned. To correct the primary cause of the event, provision the subscriber.

No Route or Trunk Group Available to Route Call - Call Processing (20)

The No Route or Trunk Group Available to Route Call event functions as a warning that there was no route or trunk group available to route a call. The primary cause of the event is that the trunk group in the route was not provisioned correctly. To correct the primary cause of the event, verify the route and trunk group provisioning.

Call Released Due to Maximum Hop Counts Exceeded - Call Processing (21)

The Call Released Due to Maximum Hop Counts Exceeded event functions as a warning that the call was released due to the maximum hop counts being exceeded. The primary cause of the event is that the number of hops between the destinations is excessive. To correct the primary cause of the event, reduce the number of hops between the destinations.

Trunk Group Index Read Failure - Call Processing (22)

The Trunk Group Index Read Failure event functions as a warning that a trunk group index read failed. The primary cause of the event is that the trunk group index could not be retrieved from the call data. To correct the primary cause of the event, check and correct the Cisco BTS 10200 Softswitch trunk group and call data provisioning.

Routing Error: Termination is Not a Subscriber - Call Processing (23)

The Routing Error: Termination is Not a Subscriber event functions as a warning that the destination termination is not a subscriber. The primary cause of the event is that the destination termination is not provisioned as a subscriber. To correct the primary cause of the event, check and correct the Cisco BTS 10200 Softswitch subscriber termination provisioning.

Invalid Route for Subscriber Index - Call Processing (24)

The Invalid Route for Subscriber Index event functions as a warning that an invalid route was selected for the subscriber index. The primary cause of the event is that the route is not provisioned correctly for the specified subscriber. To correct the primary cause of the event, check and correct the Cisco BTS 10200 Softswitch subscriber index provisioning.

Invalid Route Group for Subscriber Routing - Call Processing (25)

The Invalid Route Group for Subscriber Routing event functions as a warning that an invalid route group for the subscriber routing was selected. The primary cause of the event is that the route group is not provisioned correctly for the specified subscriber. To correct the primary cause of the event, check and correct the Cisco BTS 10200 Softswitch route group provisioning.

Invalid Trunk Group for Subscriber Routing - Call Processing (26)

The Invalid Trunk Group for Subscriber Routing event functions as a warning that an invalid trunk group for the subscriber routing was selected. The primary cause of the event is that the trunk group is not provisioned correctly for the specified subscriber. To correct the primary cause of the event, check and correct the Cisco BTS 10200 Softswitch trunk group provisioning.

Unable to Route: Blocked by Destination Subscriber Status - Call Processing (27)

The Unable to Route: Blocked by Destination Subscriber Status event functions as a warning that a call route was blocked by the destination subscriber status. The primary cause of the event is that the subscriber is not in the correct state. To correct the primary cause of the event, check and correct the Cisco BTS 10200 Softswitch subscriber state provisioning.

Route Name Does Not Exist - Call Processing (28)

The Route Name Does Not Exist event functions as a warning that the requested route name does not exist. The primary cause of the event is that the route is not provisioned correctly. To correct the primary cause of the event, check and correct the Cisco BTS 10200 Softswitch route provisioning.

Routing Selection Failure - Call Processing (29)

The Routing Selection Failure event functions as a warning that the routing selection failed. The primary cause of the event is that the route is not provisioned correctly. To correct the primary cause of the event, check and correct the Cisco BTS 10200 Softswitch route provisioning.

Customer-Originated Trace Test Failed - Call Processing (30)

The Customer-Originated Trace Test Failed event functions as a warning that the COT test failed. The primary cause of the event is that the COT test failed. To correct the primary cause of the event, contact Cisco TAC for information on how to debug the problem. Refer to the [“Obtaining Technical Assistance” section on page xxxviii](#) for detailed instructions on contacting Cisco TAC and opening a service request.

Call Authorization Failure - Call Processing (31)

The Call Authorization Failure event functions as a warning that the call authorization failed. The primary cause of the event is an provisioning error is not allowing the call to be completed. To correct the primary cause of the event, contact Cisco TAC. Refer to the [“Obtaining Technical Assistance” section on page xxxviii](#) for detailed instructions on contacting Cisco TAC and opening a service request.

Country Code Dialing Plan Error - Call Processing (32)

The Country Code Dialing Plan Error event functions as a warning that a country code dialing plan error occurred. The primary cause of the event is that the country code was not found in the dial plan. To correct the primary cause of the event, check and correct the Cisco BTS 10200 Softswitch dial plan provisioning.

Invalid Call - Call Processing (33)

The Invalid Call event functions as a warning that an invalid call was attempted. The primary cause of the event is that the call could not be completed because the number entered was invalid. To correct the primary cause of the event, check and correct the Cisco BTS 10200 Softswitch provisioning. Additionally, check the number dialed.

Dial Plan Information Not Found for Digits Received - Call Processing (34)

The Dial Plan Information Not Found for Digits Received event functions as a warning that the number entered could not be located in the dial plan. The primary cause of the event is that the Call could not be completed because the number entered could not be located in the dial plan. To correct the primary cause of the event, check and correct the Cisco BTS 10200 Softswitch dial plan provisioning. Additionally, check the number dialed.

Dial Plan Information for Test Call Not Found - Call Processing (35)

The Dial Plan Information for Test Call Not Found event functions as a warning that the test call could not be completed. The primary cause for the event is that the test call could not be completed because the number entered could not be located in the dial plan. To correct the primary cause of the event, check and correct the Cisco BTS 10200 Softswitch dial plan provisioning. Additionally, check the number tested.

Invalid or Unknown Nature of Address - Call Processing (36)

The Invalid or Unknown Nature of Address event functions as a warning that the NOA was invalid or incorrect. The primary cause of the event is that the NOA was incorrect in the dial plan. To correct the primary cause of the event, check and correct the Cisco BTS 10200 Softswitch dial plan provisioning.

Call Failure - Call Processing (37)

The Call Failure event functions as a warning that the placed call failed. The primary cause of the event is that the call failed for the reasons indicated in the data words. To correct the primary cause of the event, check the data words type of call (four bytes), calling number (20), called number (20), and failure indication (20). Once the data words are checked, contact Cisco TAC to resolve the failure indicated. Refer to the [“Obtaining Technical Assistance”](#) section on page xxxviii for detailed instructions on contacting Cisco TAC and opening a service request.

Release Cause 25 Exchange Routing Error Received - Call Processing (38)

The Release Cause 25 Exchange Routing Error Received alarm (minor) indicates that a release with cause number 25 occurred because an exchange routing error was received. To troubleshoot and correct the cause of the Release Cause 25 Exchange Routing Error Received alarm, refer to the [“Release Cause 25 Exchange Routing Error Received - Call Processing \(38\)”](#) section on page 4-29.

Test Call Blocked Due to Congestion or Isolation - Call Processing (39)

The Test Call Blocked Due to Congestion or Isolation event functions as a warning that the test call was blocked due to congestion or isolation. The primary cause of the event is that the IAM for test call was blocked due to congestion/isolation. To correct the primary cause of the event, correct congestion or isolation problem and place test call again from remote system

Troubleshooting Call Processing Alarms

This section provides the information needed to monitor and correct Calling Processing alarms.

[Table 4-3](#) lists all Calling Processing alarms in numerical order and provides cross reference to each subsection in this section.

Table 4-3 Cisco BTS 10200 Softswitch Call Processing Alarms

Alarm Type	Alarm Name	Alarm Severity
CALLP(11)	Feature Server One Link Down - Call Processing (11)	MINOR
CALLP(12)	Feature Server Both Links Down - Call Processing (12)	CRITICAL
CALLP(38)	Release Cause 25 Exchange Routing Error Received - Call Processing (38)	MINOR

Feature Server One Link Down - Call Processing (11)

The Feature Server One Link Down alarm (minor) indicates that one link to the feature server is down. The primary cause of the alarm is that the link interface hardware is broken. To correct the primary cause of the alarm, check the link interface hardware and, if necessary, reconnect or replace. The secondary cause of the alarm is that the link interface state is operationally down. To correct the secondary cause of the alarm, check the operational state of the link.

To check the operational state of the interface link and the physical condition of the interface link, proceed as follows:

- Step 1** Check status of the interface using one of the methods below (If the kstat command in Example 1 does not provide an output, try the ndd commands in example 2.):

Example 1:

```
mssol-ca0-a# kstat hme:0:hme0:link_up
module: hme                instance: 0
name:   hme0               class:   net
       link_up             1

mssol-ca0-a# kstat qfe:0:qfe0:link*
module: qfe                instance: 0
name:   qfe0               class:   net
       link_duplex         2
       link_up             1

mssol-ca0-a# kstat qfe:0:qfe0:ifspe*
module: qfe                instance: 0
name:   qfe0               class:   net
       ifspeed             100000000
```

Example 2:

```
# ndd -set /dev/eri instance 0
# ndd -get /dev/eri link_status
1
# ndd -get /dev/eri link_mode
1
# ndd -get /dev/eri link_speed
1
```

Step 2 Verify the following settings:

- Duplex should be 1 (full duplex)
- Link_up or link_status should be 1 (operational)
- Link mode should be 1 (no auto negotiation).

Step 3 Verify call agent and switch interfaces are both set to full duplex no auto negotiation.

Step 4 Verify link speed is hard-coded to the same value on both ends.

Step 5 Check for any errors pertaining to the interface in /var/adm/messages* file.

Step 6 Check operational status of ethernet interface(s) on switch side as follows:

```
admin up / line protocol up
```

Step 7 Check statistics for ethernet interface(s) on the call agent side while looking for any abnormal queue/input/output errors/collisions. For example, to check stats on bge0 interface:

```
# netstat -i -I bge0
```

```
Ipkts Ierrs Opkts Oerrs Collis Queue
```



Note

The packets queued (Queue) that cannot be transmitted should be 0. If not, it is possible that a cable or ethernet interface is defective.



Note

The input errors (Ierrs) and the output errors (Oerrs) should be close to 0. High input errors could indicate that the network is saturated, host overload, or physical network problem. High output errors could indicate a saturated local network or a bad physical connection.

Step 8 Check statistics for ethernet interface(s) on the switch side. Look for abnormal input/output errors, cyclic redundancy check (CRC), frame errors. For a description of the output of “show interface fast ethernet”, refer to:

http://www.cisco.com/en/US/customer/products/sw/iosswrel/ps1835/products_command_reference_chapter09186a00800874c4.html#wp1018148

Step 9 Paste the output of “show interfaces” to the Cisco output interpreter for further analysis of the interfaces.

<https://www.cisco.com/cgi-bin/Support/OutputInterpreter/home.pl>

Step 10 Check the physical cable, the cable connectors, and the cable connections.

Feature Server Both Links Down - Call Processing (12)

The Feature Server Both Links Down alarm (critical) indicates that both links to the feature server are down. The primary cause of the alarm is that the link interface hardware is broken. To correct the primary cause of the alarm, check the link interface hardware and, if necessary, reconnect or replace. The secondary cause of the alarm is that the link interface state is operationally down. To correct the secondary cause of the alarm, check the operational state of the link.

To check the operational state of the interface links and the physical condition of the interface links, proceed as follows:

- Step 1** Check status of the interfaces using one of the methods below (If the kstat command in Example 1 does not provide an output, try the ndd commands in example 2.):

Example 1:

```
mssol-ca0-a# kstat hme:0:hme0:link_up
module: hme                instance: 0
name:   hme0                class:   net
        link_up              1

mssol-ca0-a# kstat qfe:0:qfe0:link*
module: qfe                instance: 0
name:   qfe0                class:   net
        link_duplex          2
        link_up              1

mssol-ca0-a# kstat qfe:0:qfe0:ifspe*
module: qfe                instance: 0
name:   qfe0                class:   net
        ifspeed              100000000
```

Example 2:

```
# ndd -set /dev/eri instance 0
# ndd -get /dev/eri link_status
1
# ndd -get /dev/eri link_mode
1
# ndd -get /dev/eri link_speed
1
```

- Step 2** Verify the following settings:
- Duplex should be 1 (full duplex)
 - Link_up or link_status should be 1 (operational)
 - Link mode should be 1 (no auto negotiation).
- Step 3** Verify call agent and switch interfaces are both set to full duplex no auto negotiation.
- Step 4** Verify link speed is hard-coded to the same value on both ends.
- Step 5** Check for any errors pertaining to the interface in /var/adm/messages* file.
- Step 6** Check operational status of ethernet interface(s) on switch side as follows:
- ```
admin up / line protocol up
```



- Step 7** Check statistics for ethernet interface(s) on the call agent side while looking for any abnormal queue/input/output errors/collisions. For example, to check stats on bge0 interface:

```
netstat -i -I bge0

Ipkts Ierrs Opkts Oerrs Collis Queue
```

**Note**

The packets queued (Queue) that cannot be transmitted should be 0. If not, it is possible that a cable or ethernet interface is defective.

**Note**

The input errors (Ierrs) and the output errors (Oerrs) should be close to 0. High input errors could indicate that the network is saturated, host overload, or physical network problem. High output errors could indicate a saturated local network or a bad physical connection.

- Step 8** Check statistics for ethernet interface(s) on the switch side. Look for abnormal input/output errors, CRC, frame errors. For a description of the output of “show interface fast ethernet”, refer to:  
[http://www.cisco.com/en/US/customer/products/sw/iosswrel/ps1835/products\\_command\\_reference\\_chapter09186a00800874c4.html#wp1018148](http://www.cisco.com/en/US/customer/products/sw/iosswrel/ps1835/products_command_reference_chapter09186a00800874c4.html#wp1018148)
- Step 9** Paste the output of “show interfaces” to the Cisco output interpreter for further analysis of the interfaces.  
<https://www.cisco.com/cgi-bin/Support/OutputInterpreter/home.pl>
- Step 10** Check the physical cable, the cable connectors, and the cable connections.

## Release Cause 25 Exchange Routing Error Received - Call Processing (38)

The Release Cause 25 Exchange Routing Error Received alarm (minor) indicates that a release with cause number 25 occurred because an exchange routing error was received. The primary cause of the alarm is that a REL message with cause number 25 was received. To correct the primary cause of the alarm, log and map the cause. Refer to “[Call Authorization Failure - Call Processing \(31\)](#)” section on [page 4-24](#) for additional troubleshooting information.





## CHAPTER 5

# Configuration Troubleshooting

---

Revised: October 23, 2008, OL-11335-06

## Introduction

This chapter provides the information needed to monitor and troubleshoot Configuration events and alarms. This chapter is divided into the following sections:

- [Configuration Events and Alarms](#) – Provides a brief overview of each Configuration event and alarm.
- [Monitoring Configuration Events](#) – Provides the information needed to monitor and correct Configuration events.
- [Troubleshooting Configuration Alarms](#) – Provides the information needed to troubleshoot and correct Configuration alarms.

# Configuration Events and Alarms

This section provides a brief overview of the Configuration events and alarms for the Cisco BTS 10200 Softswitch in numerical order. [Table 5-1](#) lists all Configuration events and alarms by severity.


**Note**

Click the Configuration message number in [Table 5-1](#) to display information about the event.

**Table 5-1 Configuration Events and Alarms by Severity**

| CRITICAL                   | MAJOR                      | MINOR | WARNING | INFO                       |
|----------------------------|----------------------------|-------|---------|----------------------------|
| <a href="#">CONFIG (4)</a> | <a href="#">CONFIG (3)</a> |       |         | <a href="#">CONFIG (1)</a> |
|                            |                            |       |         | <a href="#">CONFIG (2)</a> |

## CONFIG (1)

For additional information, refer to the “[Test Report - Configuration \(1\)](#)” section on page 5-4.

|             |                    |
|-------------|--------------------|
| DESCRIPTION | Test Report        |
| SEVERITY    | Information (INFO) |
| THRESHOLD   | 10000              |
| THROTTLE    | 0                  |

## CONFIG (2)

For additional information, refer to the “[Signaling Media Gateway Adapter Wrongly Configured Domain Name - Configuration \(2\)](#)” section on page 5-4.

|                  |                                                                                                               |
|------------------|---------------------------------------------------------------------------------------------------------------|
| DESCRIPTION      | Signaling Media Gateway Adapter Wrongly Configured Domain Name (Signaling MGA Wrongly Configured Domain Name) |
| SEVERITY         | INFO                                                                                                          |
| THRESHOLD        | 1                                                                                                             |
| THROTTLE         | 1                                                                                                             |
| DATAWORDS        | Configured Domain Na - STRING [256]<br>Cause - STRING [128]                                                   |
| PRIMARY CAUSE    | Domain name is invalid.                                                                                       |
| PRIMARY ACTION   | Check domain name system (DNS) server and correct domain name.                                                |
| SECONDARY CAUSE  | At least half of the local machine address does not match Media Gateway Control Protocol (MGCP) domain name.  |
| SECONDARY ACTION | Check DNS server for domain name to ensure correct Internet Protocol (IP) address.                            |

## CONFIG (3)

To troubleshoot and correct the cause of the alarm, refer to the [“Mate Configuration Error - Configuration \(3\)” section on page 5-5](#).

|                  |                                                                             |
|------------------|-----------------------------------------------------------------------------|
| DESCRIPTION      | Keep Alive Module: Mate Configuration Error (KAM: Mate Configuration Error) |
| SEVERITY         | MAJOR                                                                       |
| THRESHOLD        | 100                                                                         |
| THROTTLE         | 0                                                                           |
| DATAWORDS        | Reason - STRING [80]                                                        |
| PRIMARY CAUSE    | Mate and local are configured to be of same side.                           |
| PRIMARY ACTION   | Configure side of the platform coming up to opposite of its mate.           |
| SECONDARY CAUSE  | Mate is configured with wrong mate Red DNS name.                            |
| SECONDARY ACTION | Configure mate DNS name properly for mate.                                  |
| TERNARY CAUSE    | Mate Red. DNS entries are changed.                                          |

## CONFIG (4)

To troubleshoot and correct the cause of the alarm, refer to the [“Configuration Error - Configuration \(4\)” section on page 5-5](#).

|                |                                                          |
|----------------|----------------------------------------------------------|
| DESCRIPTION    | Configuration Error                                      |
| SEVERITY       | CRITICAL                                                 |
| THRESHOLD      | 100                                                      |
| THROTTLE       | 0                                                        |
| DATAWORDS      | Reason - STRING [80]                                     |
| PRIMARY CAUSE  | Wrong configuration in the platform.cfg file.            |
| PRIMARY ACTION | Correct appropriate parameters in the platform.cfg file. |

# Monitoring Configuration Events

This section provides the information needed to monitor and correct Configuration events. [Table 5-2](#) lists all Configuration events in numerical order and provides cross reference to each subsection in this section.

**Table 5-2** Cisco BTS 10200 Softswitch Configuration Events

| Event Type | Event Name                                                                                         | Event Severity |
|------------|----------------------------------------------------------------------------------------------------|----------------|
| CONFIG(1)  | <a href="#">Test Report - Configuration (1)</a>                                                    | INFO           |
| CONFIG(2)  | <a href="#">Signaling Media Gateway Adapter Wrongly Configured Domain Name - Configuration (2)</a> | INFO           |
| CONFIG(3)  | <a href="#">Mate Configuration Error - Configuration (3)</a>                                       | MAJOR          |
| CONFIG(4)  | <a href="#">Configuration Error - Configuration (4)</a>                                            | CRITICAL       |

## Test Report - Configuration (1)

The Test Report event is used for testing the configuration event category. The event is informational and no further action is required.

## Signaling Media Gateway Adapter Wrongly Configured Domain Name - Configuration (2)

The Signaling Media Gateway Adapter Wrongly Configured Domain Name event functions as an informational alert that that signaling media gateway adapter (MGA) is configured with the wrong domain name. The primary cause of the event is that the domain name is invalid. To correct the primary cause of the event, check DNS server and correct domain name. The secondary cause of the event is that the at least half of the local machine address does not match the MGCP domain name. To correct secondary cause of the event, check the DNS server for the domain name to ensure that the IP address is correct.

## Mate Configuration Error - Configuration (3)

The Mate Configuration Error alarm (major) indicates that the mate configuration is incorrect. To troubleshoot and correct the cause of the Mate Configuration Error alarm, refer to the [“Mate Configuration Error - Configuration \(3\)”](#) section on page 5-5.

## Configuration Error - Configuration (4)

The Configuration Error alarm (critical) indicates that a critical configuration error has occurred. To troubleshoot and correct the cause of the Configuration Error alarm, refer to the [“Configuration Error - Configuration \(4\)”](#) section on page 5-5.

# Troubleshooting Configuration Alarms

This section provides the information needed to monitor and correct Configuration alarms. [Table 5-3](#) lists all Configuration alarms in numerical order and provides cross reference to each subsection in this section.

**Table 5-3** Cisco BTS 10200 Softswitch Configuration Alarms

| Alarm Type | Alarm Name                                                   | Alarm Severity |
|------------|--------------------------------------------------------------|----------------|
| CONFIG(3)  | <a href="#">Mate Configuration Error - Configuration (3)</a> | MAJOR          |
| CONFIG(4)  | <a href="#">Configuration Error - Configuration (4)</a>      | CRITICAL       |

## Mate Configuration Error - Configuration (3)

The Mate Configuration Error alarm (major) indicates that the mate configuration is incorrect. The primary cause of alarm is that the mate and local are configured to be of the same side. To correct the primary cause of the alarm, configure the side of the platform coming up to be the opposite of its mate. The secondary cause of the alarm is that the mate is configured with the wrong mate DNS name or the mate DNS name entries have been changed. To correct the secondary cause of the alarm, properly configure the mate DNS name.

## Configuration Error - Configuration (4)

The Configuration Error alarm (critical) indicates that a critical configuration error has occurred. The primary cause of the alarm is that there is incorrect configuration information in the platform.cfg file. To correct the primary cause of the alarm, correct the appropriate configuration parameters in the platform.cfg file.







## CHAPTER 6

# Database Troubleshooting

---

Revised: October 23, 2008, OL-11335-06

## Introduction

This chapter provides the information needed to monitor and troubleshoot Database events and alarms. This chapter is divided into the following sections:

- [Database Events and Alarms](#) – Provides a brief overview of each Database event and alarm.
- [Monitoring Database Events](#) – Provides the information needed to monitor and correct Database events.
- [Troubleshooting Database Alarms](#) – Provides the information needed to troubleshoot and correct Database alarms.

# Database Events and Alarms

This section provides a brief overview of the Database events and alarms for the Cisco BTS 10200 Softswitch in numerical order. [Table 6-1](#) lists all Database events and alarms by severity.



**Note**

Click the Database message number in [Table 6-1](#) to display information about the event or alarm.

**Table 6-1 Database Events and Alarms by Severity**

| CRITICAL                      | MAJOR                         | MINOR                         | WARNING                       | INFO                          |
|-------------------------------|-------------------------------|-------------------------------|-------------------------------|-------------------------------|
| <a href="#">DATABASE (3)</a>  | <a href="#">DATABASE (6)</a>  | <a href="#">DATABASE (7)</a>  | <a href="#">DATABASE (2)</a>  | <a href="#">DATABASE (1)</a>  |
| <a href="#">DATABASE (4)</a>  | <a href="#">DATABASE (8)</a>  | <a href="#">DATABASE (14)</a> | <a href="#">DATABASE (11)</a> | <a href="#">DATABASE (19)</a> |
| <a href="#">DATABASE (5)</a>  | <a href="#">DATABASE (10)</a> |                               | <a href="#">DATABASE (18)</a> |                               |
| <a href="#">DATABASE (9)</a>  | <a href="#">DATABASE (13)</a> |                               |                               |                               |
| <a href="#">DATABASE (12)</a> | <a href="#">DATABASE (15)</a> |                               |                               |                               |
| <a href="#">DATABASE (16)</a> | <a href="#">DATABASE (17)</a> |                               |                               |                               |
|                               | <a href="#">DATABASE (20)</a> |                               |                               |                               |

## DATABASE (1)

For additional information, refer to the “[Test Report - Database \(1\)](#)” section on page 6-15.

|             |                    |
|-------------|--------------------|
| DESCRIPTION | Test Report        |
| SEVERITY    | Information (INFO) |
| THRESHOLD   | 10000              |
| THROTTLE    | 0                  |

## DATABASE (2)

To monitor and correct the cause of the event, refer to the [“Database Management Update Failure: Master/Slave Database Out of Sync - Database \(2\)”](#) section on page 6-16.

|                  |                                                                                                                                                                                                                                                  |
|------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| DESCRIPTION      | Database Management Update Failure: Master/Slave Database Out of Sync (DBM Update Failure: Master/Slave Database Out of Synch)                                                                                                                   |
| SEVERITY         | WARNING                                                                                                                                                                                                                                          |
| THRESHOLD        | 100                                                                                                                                                                                                                                              |
| THROTTLE         | 0                                                                                                                                                                                                                                                |
| DATAWORDS        | Error Code - TWO_BYTES<br>Error String - STRING [20]<br>Provisioning String - STRING [80]                                                                                                                                                        |
| PRIMARY CAUSE    | The master database under Oracle control in the Element Management System (EMS) was successfully updated, but the subsequent update of the shared memory tables in the Call Agents (CAs) and/or Feature Servers (FSs) were not properly updated. |
| PRIMARY ACTION   | Perform an audit of the database in question to correct the data stored in shared memory.                                                                                                                                                        |
| SECONDARY ACTION | Use command line interface (CLI) to show and delete the transaction queue, and to audit and manage the queue.                                                                                                                                    |

## DATABASE (3)

To troubleshoot and correct the cause of the alarm, refer to the [“There Are Errors in Element Management System Database DefError Queue; Contact Database Administrator - Database \(3\)”](#) section on page 6-21.

|                 |                                                                                                                                                                      |
|-----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| DESCRIPTION     | There Are Errors in Element Management System Database DefError Queue; Contact Database Administrator (There are Errors in EMS Database DefError Queue; Contact DBA) |
| SEVERITY        | CRITICAL                                                                                                                                                             |
| THRESHOLD       | 100                                                                                                                                                                  |
| THROTTLE        | 0                                                                                                                                                                    |
| DATAWORDS       | Host Name - STRING [30]<br>Database Name - STRING [10]<br>Error Count - ONE_BYTE<br>Time Stamp - STRING [20]                                                         |
| PRIMARY CAUSE   | Replication data conflicts.                                                                                                                                          |
| PRIMARY ACTION  | May require manual update on database tables. Call Cisco Support. (Contact Cisco Technical Assistance Center (TAC).)                                                 |
| SECONDARY CAUSE | Update/delete on non-existing data.                                                                                                                                  |
| TERNARY CAUSE   | Unique constraint (primary key) violated.                                                                                                                            |

Refer to the [“Obtaining Technical Assistance”](#) section on page xxxviii for detailed instructions on contacting Cisco TAC and opening a service request.

## DATABASE (4)

To troubleshoot and correct the cause of the alarm, refer to the “[Element Management System Database HeartBeat: Replication PUSH Job Broken - Database \(4\)](#)” section on page 6-21.

|                  |                                                                                                                                          |
|------------------|------------------------------------------------------------------------------------------------------------------------------------------|
| DESCRIPTION      | Element Management System Database HeartBeat: Replication PUSH Job Broken (EMS DB_Heart_Beat: Replication PUSH Job Broken)               |
| SEVERITY         | CRITICAL                                                                                                                                 |
| THRESHOLD        | 100                                                                                                                                      |
| THROTTLE         | 0                                                                                                                                        |
| DATAWORDS        | Host Name - STRING [30]<br>Local Database - STRING [10]<br>Remote Database - STRING [10]<br>Job - STRING [5]<br>Time Stamp - STRING [20] |
| PRIMARY CAUSE    | Remote database is not accessible.                                                                                                       |
| PRIMARY ACTION   | Re-start up or restore remote database.                                                                                                  |
| SECONDARY CAUSE  | Remote database is down.                                                                                                                 |
| SECONDARY ACTION | Restart remote listener process.                                                                                                         |
| TERNARY CAUSE    | Remote Oracle listener process died.                                                                                                     |
| TERNARY ACTION   | Correct network connection problem.                                                                                                      |
| SUBSEQUENT CAUSE | Network connection is broken.                                                                                                            |

## DATABASE (5)

To troubleshoot and correct the cause of the alarm, refer to the [“Element Management System Database HeartBeat Process Died - Database \(5\)”](#) section on page 6-21.

|                |                                                                                                   |
|----------------|---------------------------------------------------------------------------------------------------|
| DESCRIPTION    | Element Management System Database HeartBeat Process Died (EMS DBHeartBeat Process Died)          |
| SEVERITY       | CRITICAL                                                                                          |
| THRESHOLD      | 100                                                                                               |
| THROTTLE       | 0                                                                                                 |
| DATAWORDS      | Host Name - STRING [30]<br>Database Name - STRING [10]<br>Time Stamp - STRING [20]                |
| PRIMARY CAUSE  | Terminated by the system manager program (SMG) or stopped by the platform.                        |
| PRIMARY ACTION | Restart DBHeartBeat by “dbinit -H -i start” as oracle user, or by platform start command as root. |

## DATABASE (6)

To troubleshoot and correct the cause of the alarm, refer to the [“Element Management System Database Replication DefTranDest Queue Overloaded - Database \(6\)”](#) section on page 6-22.

|                  |                                                                                                                                     |
|------------------|-------------------------------------------------------------------------------------------------------------------------------------|
| DESCRIPTION      | Element Management System Database Replication DefTranDest Queue Overloaded (EMS Database Replication DefTranDest Queue Overloaded) |
| SEVERITY         | MAJOR                                                                                                                               |
| THRESHOLD        | 100                                                                                                                                 |
| THROTTLE         | 0                                                                                                                                   |
| DATAWORDS        | Host Name - STRING [30]<br>Database Name - STRING [10]<br>Threshold - FOUR_BYTES<br>Time Stamp - STRING [20]                        |
| PRIMARY CAUSE    | Replication PUSH job is broken.                                                                                                     |
| PRIMARY ACTION   | Correct problems on remote database.                                                                                                |
| SECONDARY CAUSE  | Remote database is not accessible.                                                                                                  |
| SECONDARY ACTION | Make sure db_heart_beat process is up.                                                                                              |
| TERNARY CAUSE    | Database is overloaded.                                                                                                             |
| TERNARY ACTION   | Troubleshoot database performance.                                                                                                  |

## DATABASE (7)

To troubleshoot and correct the cause of the alarm, refer to the [“Element Management System Database DefTran Queue is Overloaded - Database \(7\)”](#) section on page 6-22.

|                  |                                                                                                             |
|------------------|-------------------------------------------------------------------------------------------------------------|
| DESCRIPTION      | Element Management System Database DefTran Queue is Overloaded (EMS Database DefTran Queue is Overloaded)   |
| SEVERITY         | MINOR                                                                                                       |
| THRESHOLD        | 100                                                                                                         |
| THROTTLE         | 0                                                                                                           |
| DATAWORDS        | Host Name - STRING [30]<br>Database Name - STRING [10]<br>Threshold - TWO_BYTES<br>Time Stamp - STRING [20] |
| PRIMARY CAUSE    | Replication DefTranDest queue is overloaded.                                                                |
| PRIMARY ACTION   | Resume replication activities.                                                                              |
| SECONDARY CAUSE  | Too many errors in DefError queue.                                                                          |
| SECONDARY ACTION | Correct replication errors.                                                                                 |
| TERNARY CAUSE    | Replication PURGE job is broken or overloaded.                                                              |
| TERNARY ACTION   | Enable replication PURGE job.                                                                               |

## DATABASE (8)

To troubleshoot and correct the cause of the alarm, refer to the [“Element Management System Database Tablespace is Out of Free Space - Database \(8\)”](#) section on page 6-22.

|                |                                                                                                                                                     |
|----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------|
| DESCRIPTION    | Element Management System Database Tablespace is Out of Free Space (EMS Database Tablespace is Out of Free Space)                                   |
| SEVERITY       | MAJOR                                                                                                                                               |
| THRESHOLD      | 100                                                                                                                                                 |
| THROTTLE       | 0                                                                                                                                                   |
| DATAWORDS      | Host Name - STRING [30]<br>Database Name - STRING [10]<br>Tablespace Name - STRING [30]<br>Total Free Space - TWO_BYTES<br>Time Stamp - STRING [20] |
| PRIMARY CAUSE  | Increased data volume or transactions.                                                                                                              |
| PRIMARY ACTION | Add more space to tablespace.                                                                                                                       |

## DATABASE (9)

To troubleshoot and correct the cause of the alarm, refer to the [“Urgent: Element Management System Database Archive Log Directory is Getting Full - Database \(9\)”](#) section on page 6-22.

|                  |                                                                                                                                               |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------|
| DESCRIPTION      | Urgent: Element Management System Database Archive Log Directory is Getting Full (URGENT: EMS Database Archive Log Directory is Getting Full) |
| SEVERITY         | CRITICAL                                                                                                                                      |
| THRESHOLD        | 100                                                                                                                                           |
| THROTTLE         | 0                                                                                                                                             |
| DATAWORDS        | Host Name - STRING [30]<br>Database Name - STRING [10]<br>Directory Name - STRING [100]<br>Free Space - TWO_BYTES<br>Time Stamp - STRING [20] |
| PRIMARY CAUSE    | Transaction volume increased.                                                                                                                 |
| PRIMARY ACTION   | Backup and cleanup archive log files.                                                                                                         |
| SECONDARY ACTION | Add more space to archive log directory.                                                                                                      |



## DATABASE (10)

To troubleshoot and correct the cause of the alarm, refer to the “[Element Management System Database: Backup Fails - Database \(10\)](#)” section on page 6-22.

|                |                                                                                                                                            |
|----------------|--------------------------------------------------------------------------------------------------------------------------------------------|
| DESCRIPTION    | Element Management System Database: Backup Fails (EMS Database: Backup Fails)                                                              |
| SEVERITY       | MAJOR                                                                                                                                      |
| THRESHOLD      | 100                                                                                                                                        |
| THROTTLE       | 0                                                                                                                                          |
| DATAWORDS      | Host Name - STRING [30]<br>Database Name - STRING [10]<br>Message 1 - STRING [200]<br>Message 2 - STRING [200]<br>Time Stamp - STRING [20] |
| PRIMARY CAUSE  | System or hardware unstable.                                                                                                               |
| PRIMARY ACTION | Re-start backup process.                                                                                                                   |

## DATABASE (11)

To troubleshoot and correct the cause of the alarm, refer to the “[Element Management System Database Alert.log Alerts - Database \(11\)](#)” section on page 6-23.

|                |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| DESCRIPTION    | Element Management System Database Alert.log Alerts (EMS Database Alert.log Alerts)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| SEVERITY       | MAJOR                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| THRESHOLD      | 100                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| THROTTLE       | 0                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| DATAWORDS      | Host Name - STRING [30]<br>Database Name - STRING [10]<br>Message 1 - STRING [200]<br>Message 2 - STRING [200]<br>Time Stamp - STRING [20]                                                                                                                                                                                                                                                                                                                                                                                                                             |
| PRIMARY CAUSE  | The probable cause of the ORA- errors report in alert.log file is documented in the \$ORACLE_HOME/rdbms/mesg/oraus.msg file. Login to EMS system as oracle user (or su - oracle) to view this file. If more information is needed, contact Cisco TAC for database support, or query Oracle Metalink library at <a href="http://metalink.oracle.com">http://metalink.oracle.com</a> .                                                                                                                                                                                   |
| PRIMARY ACTION | The corrective action is documented in the \$ORACLE_HOME/rdbms/mesg/oraus.msg file. Login to EMS system as oracle user (or su - oracle) to view this file. If more information is needed, contact Cisco TAC for database support, or query Oracle Metalink library at <a href="http://metalink.oracle.com">http://metalink.oracle.com</a> . The alert.log file is the global message file for errors issued by all Oracle background processes. The majority of error conditions may require administrator's investigation and manual correction. (Contact Cisco TAC.) |

Refer to the “[Obtaining Technical Assistance](#)” section on page xxxviii for detailed instructions on contacting Cisco TAC and opening a service request.

## DATABASE (12)

To troubleshoot and correct the cause of the alarm, refer to the [“Element Management System Database Process Died - Database \(12\)”](#) section on page 6-23.

|                  |                                                                                                                                                                                                |
|------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| DESCRIPTION      | Element Management System Database Process Died (EMS Database Process Died)                                                                                                                    |
| SEVERITY         | CRITICAL                                                                                                                                                                                       |
| THRESHOLD        | 100                                                                                                                                                                                            |
| THROTTLE         | 0                                                                                                                                                                                              |
| DATAWORDS        | Host Name - STRING [30]<br>Database Name - STRING [10]<br>Error Source - STRING [40]<br>Message - STRING [200]<br>Time Stamp - STRING [20]                                                     |
| PRIMARY CAUSE    | Possible Error Source: 1. Process Name, if local process is not running. 2. “Cannot_connect_database” if local database (DB) is unreachable. 3. “Cannot_connect_” if remote DB is unreachable. |
| PRIMARY ACTION   | Re-start process.                                                                                                                                                                              |
| SECONDARY ACTION | Contact Cisco Support. (Contact Cisco TAC.)                                                                                                                                                    |

Refer to the [“Obtaining Technical Assistance”](#) section on page xxxviii for detailed instructions on contacting Cisco TAC and opening a service request.

## DATABASE (13)

To troubleshoot and correct the cause of the alarm, refer to the [“Element Management System Database Performance Alert - Database \(13\)” section on page 6-23](#).

|                  |                                                                                                                                                                                                |
|------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| DESCRIPTION      | Element Management System Database Performance Alert (EMS Database Performance Alert)                                                                                                          |
| SEVERITY         | MAJOR                                                                                                                                                                                          |
| THRESHOLD        | 100                                                                                                                                                                                            |
| THROTTLE         | 0                                                                                                                                                                                              |
| DATAWORDS        | Host Name - STRING [30]<br>Database Name - STRING [10]<br>Stat Event Name - STRING [80]<br>Value 1 - STRING [50]<br>Value 2 - FOUR_BYTES<br>Message - STRING [200]<br>Time Stamp - STRING [20] |
| PRIMARY CAUSE    | See Stat Event Name.                                                                                                                                                                           |
| PRIMARY ACTION   | Contact Cisco Support. (Contact Cisco TAC.)                                                                                                                                                    |
| SECONDARY ACTION | Perform database performance tuning.                                                                                                                                                           |

Refer to the [“Obtaining Technical Assistance” section on page xxxviii](#) for detailed instructions on contacting Cisco TAC and opening a service request.

## DATABASE (14)

To troubleshoot and correct the cause of the alarm, refer to the [“Table Size Exceeds Minor Threshold Limit - Database \(14\)” section on page 6-23](#).

|                |                                                                                                                   |
|----------------|-------------------------------------------------------------------------------------------------------------------|
| DESCRIPTION    | Table Size Exceeds Minor Threshold Limit                                                                          |
| SEVERITY       | MINOR                                                                                                             |
| THRESHOLD      | 100                                                                                                               |
| THROTTLE       | 0                                                                                                                 |
| DATAWORDS      | Table Name - STRING [32]                                                                                          |
| PRIMARY CAUSE  | The pre-provisioned size for the stated table is nearing the licensed limit on the number of entries it can hold. |
| PRIMARY ACTION | Contact Cisco to purchase additional entry space for this particular table. (Contact Cisco TAC.)                  |

Refer to the [“Obtaining Technical Assistance” section on page xxxviii](#) for detailed instructions on contacting Cisco TAC and opening a service request.

## DATABASE (15)

To troubleshoot and correct the cause of the alarm, refer to the [“Table Size Exceeds Major Threshold Limit - Database \(15\)” section on page 6-24](#).

|                |                                          |
|----------------|------------------------------------------|
| DESCRIPTION    | Table Size Exceeds Major Threshold Limit |
| SEVERITY       | MAJOR                                    |
| THRESHOLD      | 100                                      |
| THROTTLE       | 0                                        |
| DATAWORDS      | Table Name - STRING [32]                 |
| PRIMARY CAUSE  | Major threshold limit exceeded.          |
| PRIMARY ACTION | N/A                                      |

## DATABASE (16)

To troubleshoot and correct the cause of the alarm, refer to the [“Table Size Exceeds Critical Threshold Limit - Database \(16\)” section on page 6-24](#).

|                |                                             |
|----------------|---------------------------------------------|
| DESCRIPTION    | Table Size Exceeds Critical Threshold Limit |
| SEVERITY       | CRITICAL                                    |
| THRESHOLD      | 100                                         |
| THROTTLE       | 0                                           |
| DATAWORDS      | Table Name - STRING [32]                    |
| PRIMARY CAUSE  | Critical threshold limit exceeded.          |
| PRIMARY ACTION | N/A                                         |

## DATABASE (17)

To troubleshoot and correct the cause of the alarm, refer to the [“Data Replication Failed - Database \(17\)” section on page 6-24](#).

|                 |                                                                                                           |
|-----------------|-----------------------------------------------------------------------------------------------------------|
| DESCRIPTION     | Data Replication Failed                                                                                   |
| SEVERITY        | MAJOR                                                                                                     |
| THRESHOLD       | 100                                                                                                       |
| THROTTLE        | 0                                                                                                         |
| DATAWORDS       | Replication-Stage - STRING [40]<br>Table Name - STRING [40]<br>Index - FOUR_BYTES<br>Table ID - TWO_BYTES |
| PRIMARY CAUSE   | Index out of range.                                                                                       |
| SECONDARY CAUSE | Record size mismatch.                                                                                     |

## DATABASE (18)

To monitor and correct the cause of the event, refer to the [“Unexpected Runtime Data Interaction - Database \(18\)” section on page 6-18](#).

|                |                                                                                                                                                                                                                                                                               |
|----------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| DESCRIPTION    | Unexpected Runtime Data Interaction                                                                                                                                                                                                                                           |
| SEVERITY       | WARNING                                                                                                                                                                                                                                                                       |
| THRESHOLD      | 100                                                                                                                                                                                                                                                                           |
| THROTTLE       | 0                                                                                                                                                                                                                                                                             |
| DATAWORDS      | Internal/External In - STRING [10]<br>Table Name - STRING [32]<br>Table Entry - STRING [10]<br>Table Field Name - STRING [32]<br>Descriptive Data 1 - STRING [64]<br>Descriptive Data 2 - STRING [64]<br>Descriptive Data 3 - STRING [64]<br>Descriptive Data 4 - STRING [64] |
| PRIMARY CAUSE  | Unexpected data interaction has been detected at runtime in the call agent or feature server.                                                                                                                                                                                 |
| PRIMARY ACTION | Collect logs and contact Cisco Support. (Contact Cisco TAC.)                                                                                                                                                                                                                  |

Refer to the [“Obtaining Technical Assistance” section on page xxxviii](#) for detailed instructions on contacting Cisco TAC and opening a service request.

## DATABASE (19)

For additional information, refer to the [“Daily Database Backup Completed Successfully - Database \(19\)” section on page 6-19.](#)

|                |                                                                                                                                                                  |
|----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| DESCRIPTION    | Daily Database Backup Completed Successfully                                                                                                                     |
| SEVERITY       | INFO                                                                                                                                                             |
| THRESHOLD      | 0                                                                                                                                                                |
| THROTTLE       | 0                                                                                                                                                                |
| DATAWORDS      | Host Name - STRING [60]<br>ORACLE_SID - STRING [30]<br>Process - STRING [60]<br>Message 1 - STRING [100]<br>Message 2 - STRING [100]<br>Message 3 - STRING [100] |
| PRIMARY CAUSE  | Normal operation.                                                                                                                                                |
| PRIMARY ACTION | N/A                                                                                                                                                              |

## DATABASE (20)

To troubleshoot and correct the cause of the alarm, refer to the [“Replication Data Flush Timeout During Switchover - Database \(20\)” section on page 6-24.](#)

|                |                                                                                                                                                              |
|----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------|
| DESCRIPTION    | Replication Data Flush Timeout During Switchover                                                                                                             |
| SEVERITY       | MAJOR                                                                                                                                                        |
| THRESHOLD      | 100                                                                                                                                                          |
| THROTTLE       | 0                                                                                                                                                            |
| DATAWORDS      | Tables Failed - STRING [20]                                                                                                                                  |
| PRIMARY CAUSE  | Replication module software problem.                                                                                                                         |
| PRIMARY ACTION | Database restore procedure needs to be executed on side which goes active after switchover. Alarm should be cleared manually after recovery action is taken. |

# Monitoring Database Events

This section provides the information needed to monitor and correct Database events. [Table 6-2](#) lists all Database events in numerical order and provides cross reference to each subsection in this section.

**Table 6-2** *Cisco BTS 10200 Softswitch Database Events*

| Event Type   | Event Name                                                                                                                           | Event Severity |
|--------------|--------------------------------------------------------------------------------------------------------------------------------------|----------------|
| DATABASE(1)  | <a href="#">Test Report - Database (1)</a>                                                                                           | INFO           |
| DATABASE(2)  | <a href="#">Database Management Update Failure: Master/Slave Database Out of Sync - Database (2)</a>                                 | WARNING        |
| DATABASE(3)  | <a href="#">There are Errors in Element Management System Database DefError Queue; Contact Database Administrator - Database (3)</a> | CRITICAL       |
| DATABASE(4)  | <a href="#">Element Management System Database HeartBeat: Replication PUSH Job Broken - Database (4)</a>                             | CRITICAL       |
| DATABASE(5)  | <a href="#">Element Management System Database HeartBeat Process Died - Database (5)</a>                                             | CRITICAL       |
| DATABASE(6)  | <a href="#">Element Management System Database Replication DefTranDest Queue Overloaded - Database (6)</a>                           | MAJOR          |
| DATABASE(7)  | <a href="#">Element Management System Database DefTran Queue is Overloaded - Database (7)</a>                                        | MINOR          |
| DATABASE(8)  | <a href="#">Element Management System Database Tablespace is Out of Free Space - Database (8)</a>                                    | MAJOR          |
| DATABASE(9)  | <a href="#">Urgent: Element Management System Database Archive Log Directory is Getting Full - Database (9)</a>                      | CRITICAL       |
| DATABASE(10) | <a href="#">Element Management System Database: Backup Fails - Database (10)</a>                                                     | MAJOR          |
| DATABASE(11) | <a href="#">Element Management System Database Alert.log Alerts - Database (11)</a>                                                  | MAJOR          |
| DATABASE(12) | <a href="#">Element Management System Database Process Died - Database (12)</a>                                                      | CRITICAL       |
| DATABASE(13) | <a href="#">Element Management System Database Performance Alert - Database (13)</a>                                                 | MAJOR          |
| DATABASE(14) | <a href="#">Table Size Exceeds Minor Threshold Limit - Database (14)</a>                                                             | MINOR          |
| DATABASE(15) | <a href="#">Table Size Exceeds Major Threshold Limit - Database (15)</a>                                                             | MAJOR          |
| DATABASE(16) | <a href="#">Table Size Exceeds Critical Threshold Limit - Database (16)</a>                                                          | CRITICAL       |
| DATABASE(17) | <a href="#">Data Replication Failed - Database (17)</a>                                                                              | MAJOR          |
| DATABASE(18) | <a href="#">Unexpected Runtime Data Interaction - Database (18)</a>                                                                  | WARNING        |
| DATABASE(19) | <a href="#">Daily Database Backup Completed Successfully - Database (19)</a>                                                         | INFO           |
| DATABASE(20) | <a href="#">Replication Data Flush Timeout During Switchover - Database (20)</a>                                                     | MAJOR          |

## Test Report - Database (1)

The Test Report is for testing the database event category. The event is informational and no further action is required.

## Database Management Update Failure: Master/Slave Database Out of Sync - Database (2)

The Database Management Update Failure: Master/Slave Database Out of Sync event functions as a warning that master and slave databases are out of sync. The primary cause of the event is that the master database under Oracle control in the EMS was successfully updated, but the subsequent update of the shared memory tables in the Call Agent (CA) servers and/or Feature Servers (FS) were not properly updated. To correct the primary cause of the event, perform an audit of the database in question to correct the data stored in shared memory. Additionally, use the CLI to show and delete the transaction queue, and to audit and manage the queue.

## There are Errors in Element Management System Database DefError Queue; Contact Database Administrator - Database (3)

The There are Errors in Element Management System Database DefError Queue; Contact Database Administrator alarm (critical) indicates that there are errors in the EMS database DefError queue. To troubleshoot and correct the cause of the There are Errors in Element Management System Database DefError Queue; Contact Database Administrator alarm, refer to the [“There Are Errors in Element Management System Database DefError Queue; Contact Database Administrator - Database \(3\)”](#) section on page 6-21.

## Element Management System Database HeartBeat: Replication PUSH Job Broken - Database (4)

The Element Management System Database HeartBeat: Replication PUSH Job Broken alarm (critical) indicates that the replication PUSH job is broken. To troubleshoot and correct the cause of the of the Element Management System Database HeartBeat: Replication PUSH Job Broken alarm, refer to the [“Element Management System Database HeartBeat: Replication PUSH Job Broken - Database \(4\)”](#) section on page 6-21.

## Element Management System Database HeartBeat Process Died - Database (5)

The Element Management System Database HeartBeat Process Died alarm (critical) indicates that the EMS database heartbeat process has died. To troubleshoot and correct the cause of the Element Management System Database HeartBeat Process Died alarm, refer to the [“Element Management System Database HeartBeat Process Died - Database \(5\)”](#) section on page 6-21.

## Element Management System Database Replication DefTranDest Queue Overloaded - Database (6)

The Element Management System Database Replication DefTranDest Queue Overloaded alarm (major) indicates that the EMS database replication DefTranDest queue is overloaded. To troubleshoot and correct the cause of the Element Management System Database Replication DefTranDest Queue Overloaded alarm, refer to the [“Element Management System Database Replication DefTranDest Queue Overloaded - Database \(6\)”](#) section on page 6-22.



## Element Management System Database DefTran Queue is Overloaded - Database (7)

The Element Management System Database DefTran Queue is Overloaded alarm (minor) indicates that the EMS database DefTran queue is overloaded. To troubleshoot and correct the cause of the Element Management System Database DefTran Queue is Overloaded alarm, refer to the [“Element Management System Database DefTran Queue is Overloaded - Database \(7\)”](#) section on page 6-22.

## Element Management System Database Tablespace is Out of Free Space - Database (8)

The Element Management System Database Tablespace is Out of Free Space alarm (major) indicates that the EMS database table space is out of free space. To troubleshoot and correct the cause of the Element Management System Database Tablespace is Out of Free Space alarm, refer to the [“Element Management System Database Tablespace is Out of Free Space - Database \(8\)”](#) section on page 6-22.

## Urgent: Element Management System Database Archive Log Directory is Getting Full - Database (9)

The Urgent: Element Management System Database Archive Log Directory is Getting Full alarm (critical) indicates that the EMS database archive log directory is getting full. To troubleshoot and correct the cause of the Urgent: Element Management System Database Archive Log Directory is Getting Full alarm, refer to the [“Urgent: Element Management System Database Archive Log Directory is Getting Full - Database \(9\)”](#) section on page 6-22.

## Element Management System Database: Backup Fails - Database (10)

The Element Management System Database: Backup Fails alarm (major) indicates that the EMS database backup has failed. To troubleshoot and correct the cause of the Element Management System Database: Backup Fails alarm, refer to the [“Element Management System Database: Backup Fails - Database \(10\)”](#) section on page 6-22.

## Element Management System Database Alert.log Alerts - Database (11)

The Element Management System Database Alert.log Alerts alarm (major) indicates that the EMS database alerts are being received and logged into the alert log. To troubleshoot and correct the cause of the Element Management System Database Alert.log Alerts alarm, refer to the [“Element Management System Database Alert.log Alerts - Database \(11\)”](#) section on page 6-23.

## Element Management System Database Process Died - Database (12)

The Element Management System Database Process Died alarm (critical) indicates that the EMS database process has died. To troubleshoot and correct the cause of the Element Management System Database Process Died alarm, refer to the [“Element Management System Database Process Died - Database \(12\)”](#) section on page 6-23.

## Element Management System Database Performance Alert - Database (13)

The Element Management System Database Performance Alert alarm (major) indicates that the EMS database performance has degraded. To troubleshoot and correct the cause of the Element Management System Database Performance Alert alarm, refer to the [“Element Management System Database Performance Alert - Database \(13\)”](#) section on page 6-23.

## Table Size Exceeds Minor Threshold Limit - Database (14)

The Table Size Exceeds Minor Threshold Limit alarm (minor) indicates that the table size has exceeded the minor threshold crossing limit. To troubleshoot and correct the cause of the Table Size Exceeds Minor Threshold Limit alarm, refer to the [“Table Size Exceeds Minor Threshold Limit - Database \(14\)”](#) section on page 6-23.

## Table Size Exceeds Major Threshold Limit - Database (15)

The Table Size Exceeds Major Threshold Limit alarm (major) indicates that the table size has exceeded the major threshold crossing limit. To troubleshoot and correct the cause of the Table Size Exceeds Major Threshold Limit alarm, refer to the [“Table Size Exceeds Major Threshold Limit - Database \(15\)”](#) section on page 6-24.

## Table Size Exceeds Critical Threshold Limit - Database (16)

The Table Size Exceeds Critical Threshold Limit alarm (critical) indicates that the table size has exceeded the critical threshold crossing limit. To troubleshoot and correct the cause of the Table Size Exceeds Critical Threshold Limit alarm, refer to the [“Table Size Exceeds Critical Threshold Limit - Database \(16\)”](#) section on page 6-24.

## Data Replication Failed - Database (17)

The Data Replication Failed alarm (major) indicates that the data replication failed. To troubleshoot and correct the cause of the Data Replication Failed alarm, refer to the [“Data Replication Failed - Database \(17\)”](#) section on page 6-24.

## Unexpected Runtime Data Interaction - Database (18)

The Unexpected Runtime Data Interaction event functions as a warning that an unexpected runtime data interaction has occurred. The primary cause of the event is that an unexpected data interaction has been detected at runtime in the call agent or feature server. To correct the primary cause of the event, collect the logs and contact Cisco TAC. Refer to the [“Obtaining Technical Assistance”](#) section on page xxxviii for detailed instructions on contacting Cisco TAC and opening a service request.

## Daily Database Backup Completed Successfully - Database (19)

The Daily Database Backup Completed Successfully event functions as an informational alert that the daily database backup has completed successfully. The event is informational and no further action is required.

## Replication Data Flush Timeout During Switchover - Database (20)

The Replication Data Flush Timeout During Switchover alarm (major) indicates that the replication data flush timed out during a switchover. To troubleshoot and correct the cause of the Replication Data Flush Timeout During Switchover alarm, refer to the [“Replication Data Flush Timeout During Switchover - Database \(20\)”](#) section on page 6-24.

# Troubleshooting Database Alarms

This section provides the information needed to monitor and correct Database alarms. [Table 6-3](#) lists all Database alarms in numerical order and provides cross reference to each subsection in this section.

**Table 6-3** *Cisco BTS 10200 Softswitch Database Alarms*

| Alarm Type   | Alarm Name                                                                                                                           | Alarm Severity |
|--------------|--------------------------------------------------------------------------------------------------------------------------------------|----------------|
| DATABASE(3)  | <a href="#">There Are Errors in Element Management System Database DefError Queue; Contact Database Administrator - Database (3)</a> | CRITICAL       |
| DATABASE(4)  | <a href="#">Element Management System Database HeartBeat: Replication PUSH Job Broken - Database (4)</a>                             | CRITICAL       |
| DATABASE(5)  | <a href="#">Element Management System Database HeartBeat Process Died - Database (5)</a>                                             | CRITICAL       |
| DATABASE(6)  | <a href="#">Element Management System Database Replication DefTranDest Queue Overloaded - Database (6)</a>                           | MAJOR          |
| DATABASE(7)  | <a href="#">Element Management System Database DefTran Queue is Overloaded - Database (7)</a>                                        | MINOR          |
| DATABASE(8)  | <a href="#">Element Management System Database Tablespace is Out of Free Space - Database (8)</a>                                    | MAJOR          |
| DATABASE(9)  | <a href="#">Urgent: Element Management System Database Archive Log Directory is Getting Full - Database (9)</a>                      | CRITICAL       |
| DATABASE(10) | <a href="#">Element Management System Database: Backup Fails - Database (10)</a>                                                     | MAJOR          |
| DATABASE(11) | <a href="#">Element Management System Database Alert.log Alerts - Database (11)</a>                                                  | MAJOR          |
| DATABASE(12) | <a href="#">Element Management System Database Process Died - Database (12)</a>                                                      | CRITICAL       |
| DATABASE(13) | <a href="#">Element Management System Database Performance Alert - Database (13)</a>                                                 | MAJOR          |
| DATABASE(14) | <a href="#">Table Size Exceeds Minor Threshold Limit - Database (14)</a>                                                             | MINOR          |
| DATABASE(15) | <a href="#">Table Size Exceeds Major Threshold Limit - Database (15)</a>                                                             | MAJOR          |
| DATABASE(16) | <a href="#">Table Size Exceeds Critical Threshold Limit - Database (16)</a>                                                          | CRITICAL       |
| DATABASE(17) | <a href="#">Data Replication Failed - Database (17)</a>                                                                              | MAJOR          |
| DATABASE(20) | <a href="#">Replication Data Flush Timeout During Switchover - Database (20)</a>                                                     | MAJOR          |

## There Are Errors in Element Management System Database DefError Queue; Contact Database Administrator - Database (3)

The There Are Errors in Element Management System Database DefError Queue; Contact Database Administrator alarm (critical) indicates that there are errors in the EMS database DefError queue. The primary cause of the alarm is that replication data conflicts have occurred. The additional causes of the alarm are that a request for update or delete on non-existing data occurred, or an unique constraint (primary key) was violated. Correcting the cause of the alarm may require a manual update on database tables. Contact Cisco TAC for assistance. Refer to the [“Obtaining Technical Assistance” section on page xxxviii](#) for detailed instructions on contacting Cisco TAC and opening a service request.

Prior to opening the Cisco TAC service request, take the following steps:

- 
- Step 1** Login to the EMS reported in the “Hostname” dataword and execute the following commands and collect the reported information.

```
su - oracle
dbadm -C rep
dbadm -r get_deferror
dbadm -r get_defcall_order
```

- Step 2** Check the collected information against any known field notices at the following link:

[http://www.cisco.com/en/US/products/hw/vcallcon/ps531/prod\\_field\\_notices\\_list.html](http://www.cisco.com/en/US/products/hw/vcallcon/ps531/prod_field_notices_list.html)

---

## Element Management System Database HeartBeat: Replication PUSH Job Broken - Database (4)

The Element Management System Database HeartBeat: Replication PUSH Job Broken alarm (critical) indicates that the replication PUSH job is broken. The primary cause of the alarm is that the remote database is down or the remote database is not accessible. To correct the primary cause of the alarm, re-start or restore remote database. The secondary cause of the alarm is that network connections in broken. To correct the secondary cause of the alarm, correct the network connection problem. The ternary cause of the alarm is that the remote Oracle Listener process died. To correct the ternary cause of the alarm, restart the remote Listener process.

## Element Management System Database HeartBeat Process Died - Database (5)

The Element Management System Database HeartBeat Process Died alarm (critical) indicates that the EMS database heartbeat process has died. The primary cause of the alarm is that the EMS DBHeartBeat Process was terminated by SMG, or stopped by the platform. To correct the primary cause of the alarm, restart the DBHeartBeat by executing the “dbinit -H -i start” command as an Oracle user, or by executing the platform start command as a root user.

## Element Management System Database Replication DefTranDest Queue Overloaded - Database (6)

The Element Management System Database Replication DefTranDest Queue Overloaded alarm (major) indicates that the EMS database replication DefTranDest queue is overloaded. The primary cause of the alarm is that the replication PUSH job is broken. To correct the primary cause of the alarm, correct the problems on remote database. The secondary cause of the alarm is that the remote database is not accessible. To correct the secondary cause of the alarm, verify that the db\_heart\_beat process is up. The ternary cause of the alarm is that the database is overloaded. To correct the ternary cause of the alarm, troubleshoot database performance.

## Element Management System Database DefTran Queue is Overloaded - Database (7)

The Element Management System Database DefTran Queue is Overloaded alarm (minor) indicates that the EMS database DefTran queue is overloaded. The primary cause of the alarm is that the replication DefTranDest queue is overloaded. To correct the primary cause of the alarm, resume replication activities. The secondary cause of the alarm is that there are too many errors in DefError queue. To correct the secondary cause of the alarm, correct the replication errors. The ternary cause of the alarm is the replication PURGE job is broken or overloaded. To correct the ternary cause of the alarm, enable the replication PURGE job.

## Element Management System Database Tablespace is Out of Free Space - Database (8)

The Element Management System Database Tablespace is Out of Free Space alarm (major) indicates that the EMS database table space is out of free space. The primary cause of the alarm is that there has been an increase in data volume or transactions. To correct the primary cause of the alarm, add more space to the tablespace.

## Urgent: Element Management System Database Archive Log Directory is Getting Full - Database (9)

The Urgent: Element Management System Database Archive Log Directory is Getting Full alarm (critical) indicates that the EMS database archive log directory is getting full. The primary cause of the alarm is that transaction volume has increased. To correct the primary cause of the alarm, backup and cleanup the archive log files. Additionally, add more space to archive log directory.

## Element Management System Database: Backup Fails - Database (10)

The Element Management System Database: Backup Fails alarm (major) indicates that the EMS database backup has failed. The primary cause of the alarm is that the system or hardware is unstable. To correct the primary cause of the alarm, re-start the backup process.

## Element Management System Database Alert.log Alerts - Database (11)

The Element Management System Database Alert.log Alerts alarm (major) indicates that the EMS database alerts are being received and logged into the alert log. The probable cause of the ORA- error reported in this event is documented in the \$ORACLE\_HOME/rdbms/mesg/oraus.msg file. Login to EMS system as oracle user (or su - oracle) to view this file. If more information is needed, contact Cisco TAC support, or query Oracle Metalink library at <http://metalink.oracle.com>. The corrective action is documented in the \$ORACLE\_HOME/rdbms/mesg/oraus.msg file. To view the file, login to EMS system as root, then su - oracle. After the situation is corrected, user will need to manually clear this event. This event does not automatically clear the alarm. If further support is needed, contact Cisco TAC support, or query Oracle Metalink library at <http://metalink.oracle.com>. Refer to the [“Obtaining Technical Assistance” section on page xxxviii](#) for detailed instructions on contacting Cisco TAC and opening a service request.

## Element Management System Database Process Died - Database (12)

The Element Management System Database Process Died alarm (critical) indicates that the EMS database process has died. The primary possible causes of the alarm are:

- Process Name, if local process is not running.
- “Cannot\_connect\_database” if local DB is unreachable.
- “Cannot\_connect\_” if remote DB is unreachable.

To correct the possible causes of the alarm, re-start process and contact Cisco TAC. Refer to the [“Obtaining Technical Assistance” section on page xxxviii](#) for detailed instructions on contacting Cisco TAC and opening a service request.

## Element Management System Database Performance Alert - Database (13)

The Element Management System Database Performance Alert alarm (major) indicates that the EMS database performance has degraded. To identify the primary cause of the alarm, check the “StatEventName” dataword information. To correct the primary cause of the alarm, perform database performance tuning and contact Cisco TAC. Refer to the [“Obtaining Technical Assistance” section on page xxxviii](#) for detailed instructions on contacting Cisco TAC and opening a service request.

## Table Size Exceeds Minor Threshold Limit - Database (14)

The Table Size Exceeds Minor Threshold Limit alarm (minor) indicates that the table size has exceeded the minor threshold crossing limit. The primary cause of the alarm is that the pre-provisioned size for the stated table is nearing the licensed limit on the number of entries it can hold. To correct the primary cause of the alarm, contact Cisco TAC to purchase additional entry space for this particular table. Refer to the [“Obtaining Technical Assistance” section on page xxxviii](#) for detailed instructions on contacting Cisco TAC and opening a service request.

## Table Size Exceeds Major Threshold Limit - Database (15)

The Table Size Exceeds Major Threshold Limit alarm (major) indicates that the table size has exceeded the major threshold crossing limit. The primary cause of the Table Size Exceeds Major Threshold Limit alarm is the major threshold crossing limit has been exceeded. No further action is required.

## Table Size Exceeds Critical Threshold Limit - Database (16)

The Table Size Exceeds Critical Threshold Limit alarm (critical) indicates that the table size has exceeded the critical threshold crossing limit. The primary cause of the alarm is that the critical threshold limit was exceeded. No corrective action is required.

## Data Replication Failed - Database (17)

The Data Replication Failed alarm (major) indicates that the data replication failed. The primary cause of the alarm is that an index is out of range. The secondary cause of the alarm is that a record size mismatch occurred. No corrective action is required.

## Replication Data Flush Timeout During Switchover - Database (20)

The Replication Data Flush Timeout During Switchover alarm (major) indicates that the replication data flush timed out during a switchover. The primary cause of the alarm is that a Replication Module software problem has occurred. To correct the primary cause of the alarm, a database restore procedure needs to be executed on the side which goes active after a switchover. The alarm should be cleared manually after recovery action is taken.





## CHAPTER 7

# Maintenance Troubleshooting

---

Revised: October 23, 2008, OL-11335-06

## Introduction

This chapter provides the information needed to monitor and troubleshoot Maintenance events and alarms. This chapter is divided into the following sections:

- [Maintenance Events and Alarms](#) – Provides a brief overview of each Maintenance event and alarm.
- [Monitoring Maintenance Events](#) – Provides the information needed to monitor and correct Maintenance events.
- [Troubleshooting Maintenance Alarms](#) – Provides the information needed to troubleshoot and correct Maintenance alarms.

# Maintenance Events and Alarms

This section provides a brief overview of the Maintenance events and alarms for the Cisco BTS 10200 Softswitch in numerical order. [Table 7-1](#) lists all maintenance events and alarms by severity.


**Note**

Click the maintenance message number in [Table 7-1](#) to display information about the event.

**Table 7-1** Maintenance Events and Alarms by Severity

| CRITICAL                          | MAJOR                            | MINOR                            | WARNING                          | INFO                             |
|-----------------------------------|----------------------------------|----------------------------------|----------------------------------|----------------------------------|
| <a href="#">MAINTENANCE (40)</a>  | <a href="#">MAINTENANCE (3)</a>  | <a href="#">MAINTENANCE (18)</a> | <a href="#">MAINTENANCE (29)</a> | <a href="#">MAINTENANCE (1)</a>  |
| <a href="#">MAINTENANCE (43)</a>  | <a href="#">MAINTENANCE (4)</a>  | <a href="#">MAINTENANCE (24)</a> | <a href="#">MAINTENANCE (41)</a> | <a href="#">MAINTENANCE (2)</a>  |
| <a href="#">MAINTENANCE (44)</a>  | <a href="#">MAINTENANCE (5)</a>  | <a href="#">MAINTENANCE (48)</a> | <a href="#">MAINTENANCE (75)</a> | <a href="#">MAINTENANCE (11)</a> |
| <a href="#">MAINTENANCE (47)</a>  | <a href="#">MAINTENANCE (6)</a>  | <a href="#">MAINTENANCE (67)</a> |                                  | <a href="#">MAINTENANCE (12)</a> |
| <a href="#">MAINTENANCE (50)</a>  | <a href="#">MAINTENANCE (7)</a>  | <a href="#">MAINTENANCE (83)</a> |                                  | <a href="#">MAINTENANCE (13)</a> |
| <a href="#">MAINTENANCE (53)</a>  | <a href="#">MAINTENANCE (8)</a>  | <a href="#">MAINTENANCE (86)</a> |                                  | <a href="#">MAINTENANCE (14)</a> |
| <a href="#">MAINTENANCE (57)</a>  | <a href="#">MAINTENANCE (9)</a>  | <a href="#">MAINTENANCE (90)</a> |                                  | <a href="#">MAINTENANCE (15)</a> |
| <a href="#">MAINTENANCE (61)</a>  | <a href="#">MAINTENANCE (10)</a> | <a href="#">MAINTENANCE (98)</a> |                                  | <a href="#">MAINTENANCE (16)</a> |
| <a href="#">MAINTENANCE (65)</a>  | <a href="#">MAINTENANCE (19)</a> |                                  |                                  | <a href="#">MAINTENANCE (17)</a> |
| <a href="#">MAINTENANCE (69)</a>  | <a href="#">MAINTENANCE (20)</a> |                                  |                                  | <a href="#">MAINTENANCE (22)</a> |
| <a href="#">MAINTENANCE (70)</a>  | <a href="#">MAINTENANCE (21)</a> |                                  |                                  | <a href="#">MAINTENANCE (25)</a> |
| <a href="#">MAINTENANCE (73)</a>  | <a href="#">MAINTENANCE (23)</a> |                                  |                                  | <a href="#">MAINTENANCE (27)</a> |
| <a href="#">MAINTENANCE (74)</a>  | <a href="#">MAINTENANCE (26)</a> |                                  |                                  | <a href="#">MAINTENANCE (28)</a> |
| <a href="#">MAINTENANCE (82)</a>  | <a href="#">MAINTENANCE (42)</a> |                                  |                                  | <a href="#">MAINTENANCE (30)</a> |
| <a href="#">MAINTENANCE (85)</a>  | <a href="#">MAINTENANCE (45)</a> |                                  |                                  | <a href="#">MAINTENANCE (32)</a> |
| <a href="#">MAINTENANCE (91)</a>  | <a href="#">MAINTENANCE (49)</a> |                                  |                                  | <a href="#">MAINTENANCE (33)</a> |
| <a href="#">MAINTENANCE (97)</a>  | <a href="#">MAINTENANCE (51)</a> |                                  |                                  | <a href="#">MAINTENANCE (34)</a> |
| <a href="#">MAINTENANCE (100)</a> | <a href="#">MAINTENANCE (55)</a> |                                  |                                  | <a href="#">MAINTENANCE (35)</a> |
| <a href="#">MAINTENANCE (101)</a> | <a href="#">MAINTENANCE (62)</a> |                                  |                                  | <a href="#">MAINTENANCE (36)</a> |
| <a href="#">MAINTENANCE (102)</a> | <a href="#">MAINTENANCE (63)</a> |                                  |                                  | <a href="#">MAINTENANCE (37)</a> |
| <a href="#">MAINTENANCE (103)</a> | <a href="#">MAINTENANCE (64)</a> |                                  |                                  | <a href="#">MAINTENANCE (38)</a> |
|                                   | <a href="#">MAINTENANCE (66)</a> |                                  |                                  | <a href="#">MAINTENANCE (39)</a> |
|                                   | <a href="#">MAINTENANCE (68)</a> |                                  |                                  | <a href="#">MAINTENANCE (46)</a> |
|                                   | <a href="#">MAINTENANCE (71)</a> |                                  |                                  | <a href="#">MAINTENANCE (52)</a> |
|                                   | <a href="#">MAINTENANCE (72)</a> |                                  |                                  | <a href="#">MAINTENANCE (54)</a> |
|                                   | <a href="#">MAINTENANCE (77)</a> |                                  |                                  | <a href="#">MAINTENANCE (56)</a> |
|                                   | <a href="#">MAINTENANCE (84)</a> |                                  |                                  | <a href="#">MAINTENANCE (58)</a> |
|                                   | <a href="#">MAINTENANCE (87)</a> |                                  |                                  | <a href="#">MAINTENANCE (78)</a> |
|                                   | <a href="#">MAINTENANCE (88)</a> |                                  |                                  | <a href="#">MAINTENANCE (79)</a> |
|                                   | <a href="#">MAINTENANCE (89)</a> |                                  |                                  | <a href="#">MAINTENANCE (80)</a> |
|                                   | <a href="#">MAINTENANCE (92)</a> |                                  |                                  | <a href="#">MAINTENANCE (81)</a> |

**Table 7-1** Maintenance Events and Alarms by Severity (continued)

| CRITICAL | MAJOR                            | MINOR | WARNING | INFO                             |
|----------|----------------------------------|-------|---------|----------------------------------|
|          | <a href="#">MAINTENANCE (93)</a> |       |         | <a href="#">MAINTENANCE (94)</a> |
|          | <a href="#">MAINTENANCE (99)</a> |       |         | <a href="#">MAINTENANCE (95)</a> |
|          |                                  |       |         | <a href="#">MAINTENANCE (96)</a> |

## MAINTENANCE (1)

For additional information, refer to the [“Test Report - Maintenance \(1\)”](#) section on page 7-58.

|             |                    |
|-------------|--------------------|
| DESCRIPTION | Test Report        |
| SEVERITY    | Information (INFO) |
| THRESHOLD   | 10000              |
| THROTTLE    | 0                  |

## MAINTENANCE (2)

For additional information, refer to the [“Report Threshold Exceeded - Maintenance \(2\)”](#) section on page 7-58.

|                |                                                                                                                                                                                   |
|----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| DESCRIPTION    | Report Threshold Exceeded                                                                                                                                                         |
| SEVERITY       | INFO                                                                                                                                                                              |
| THRESHOLD      | 0                                                                                                                                                                                 |
| THROTTLE       | 0                                                                                                                                                                                 |
| DATAWORDS      | Report Type - TWO_BYTES<br>Report Number - TWO_BYTES<br>Threshold Level - TWO_BYTES                                                                                               |
| PRIMARY CAUSE  | Issued when the threshold for a given report type and number is exceeded.                                                                                                         |
| PRIMARY ACTION | No action is required since this is an information report. The root cause event report - threshold should be investigated to determine if there is a service affecting situation. |

## MAINTENANCE (3)

To troubleshoot and correct the cause of the alarm, refer to the [“Local Side has Become Faulty - Maintenance \(3\)” section on page 7-77](#).

|                  |                                                                                                                                                                                        |
|------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| DESCRIPTION      | Keep Alive Module: Local Side has Become Faulty (KAM: Local Side Has Become Faulty)                                                                                                    |
| SEVERITY         | MAJOR                                                                                                                                                                                  |
| THRESHOLD        | 100                                                                                                                                                                                    |
| THROTTLE         | 0                                                                                                                                                                                      |
| DATAWORDS        | Local State - STRING [30]<br>Mate State - STRING [30]<br>Reason - STRING [80]<br>Probable Cause - STRING [80]                                                                          |
| PRIMARY CAUSE    | Can result from maintenance report 5, 6, 9, 10, 19, 20.                                                                                                                                |
| PRIMARY ACTION   | Review information from command line interface (CLI) log report. Usually software problem; restart software using the installation and startup procedure.                              |
| SECONDARY CAUSE  | Manually shutting down the system using platform stop command.                                                                                                                         |
| SECONDARY ACTION | Reboot host machine, reinstall all applications and restart all applications. If fault state is a commonly occurring problem, then operating system (OS) or hardware may be a problem. |

## MAINTENANCE (4)

To troubleshoot and correct the cause of the alarm, refer to the [“Mate Side has Become Faulty - Maintenance \(4\)”](#) section on page 7-77.

|                   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|-------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| DESCRIPTION       | Keep Alive Module: Mate Side Has Become Faulty (KAM: Mate Side Has Become Faulty)                                                                                                                                                                                                                                                                                                                                                                                                      |
| SEVERITY          | MAJOR                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| THRESHOLD         | 100                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| THROTTLE          | 0                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| DATAWORDS         | Local State - STRING [30]<br>Mate State - STRING [30]<br>Reason - STRING [80]<br>Probable Cause - STRING [80]<br>Mate Ping - STRING [50]                                                                                                                                                                                                                                                                                                                                               |
| PRIMARY CAUSE     | Local side has detected the mate side going to faulty state.                                                                                                                                                                                                                                                                                                                                                                                                                           |
| PRIMARY ACTION    | Display the event summary on the faulty mate side, using the report event-summary command (see the CLI Guide for command details).                                                                                                                                                                                                                                                                                                                                                     |
| SECONDARY ACTION  | Review information in the event summary. This is usually a software problem.                                                                                                                                                                                                                                                                                                                                                                                                           |
| TERNARY ACTION    | After confirming the active side is processing traffic, restart software on the mate side. Log in to the mate platform as root user. Enter platform stop command and then platform start command.                                                                                                                                                                                                                                                                                      |
| SUBSEQUENT ACTION | If software restart does not resolve the problem that is, if the platform goes immediately to faulty again, or does not start, contact Cisco Technical Assistance Center (TAC). It may be necessary to reinstall software. If problem is commonly occurring, then OS or hardware may be a problem. Reboot host machine, then reinstall and restart all applications. If you reboot, this will bring down other applications running on this machine. Contact Cisco TAC for assistance. |

Refer to the [“Obtaining Technical Assistance”](#) section on page xxxviii for detailed instructions on contacting Cisco TAC and opening a service request.

## MAINTENANCE (5)

To troubleshoot and correct the cause of the alarm, refer to the [“Changeover Failure - Maintenance \(5\)” section on page 7-77](#).

|                   |                                                                                                                                                                                                                                                                                                                                                                          |
|-------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| DESCRIPTION       | Keep Alive Module: Changeover Failure (KAM: Changeover Failure)                                                                                                                                                                                                                                                                                                          |
| SEVERITY          | MAJOR                                                                                                                                                                                                                                                                                                                                                                    |
| THRESHOLD         | 100                                                                                                                                                                                                                                                                                                                                                                      |
| THROTTLE          | 0                                                                                                                                                                                                                                                                                                                                                                        |
| DATAWORDS         | Local State - STRING [30]<br>Mate State - STRING [30]                                                                                                                                                                                                                                                                                                                    |
| PRIMARY CAUSE     | Issued when changing from an active processor to a standby and the changeover fails.                                                                                                                                                                                                                                                                                     |
| PRIMARY ACTION    | Review information from CLI log report.                                                                                                                                                                                                                                                                                                                                  |
| SECONDARY CAUSE   | This alarm is usually caused by a software problem on the specific platform identified in the alarm report.                                                                                                                                                                                                                                                              |
| SECONDARY ACTION  | On the platform identified in this alarm report, restart the platform.                                                                                                                                                                                                                                                                                                   |
| TERNARY ACTION    | If platform restart is not successful, reinstall the application for this platform, and then restart platform again.                                                                                                                                                                                                                                                     |
| SUBSEQUENT ACTION | If necessary, reboot host machine this platform is located on. Then reinstall and restart all applications on this machine. If faulty state is a commonly occurring event, then OS or hardware may be a problem. Contact Cisco TAC for assistance. It may also be helpful to gather information event/alarm reports that were issued before and after this alarm report. |

Refer to the [“Obtaining Technical Assistance” section on page xxxviii](#) for detailed instructions on contacting Cisco TAC and opening a service request.

## MAINTENANCE (6)

To troubleshoot and correct the cause of the alarm, refer to the [“Changeover Timeout - Maintenance \(6\)” section on page 7-78](#).

|                   |                                                                                                                                                                                                                                                                                                                                                                                                 |
|-------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| DESCRIPTION       | Keep Alive Module: Changeover Timeout (KAM: Changeover Timeout)                                                                                                                                                                                                                                                                                                                                 |
| SEVERITY          | MAJOR                                                                                                                                                                                                                                                                                                                                                                                           |
| THRESHOLD         | 100                                                                                                                                                                                                                                                                                                                                                                                             |
| THROTTLE          | 0                                                                                                                                                                                                                                                                                                                                                                                               |
| DATAWORDS         | Local State - STRING [30]<br>Mate State - STRING [30]                                                                                                                                                                                                                                                                                                                                           |
| PRIMARY CAUSE     | System failed to changeover within time period. Soon after this event is issued, one platform will go to faulty state.                                                                                                                                                                                                                                                                          |
| PRIMARY ACTION    | Review information from CLI log report.                                                                                                                                                                                                                                                                                                                                                         |
| SECONDARY CAUSE   | This alarm is usually caused by a software problem on the specific platform identified in the alarm report.                                                                                                                                                                                                                                                                                     |
| SECONDARY ACTION  | On the platform identified in this alarm report, restart the platform.                                                                                                                                                                                                                                                                                                                          |
| TERNARY ACTION    | If platform restart is not successful, reinstall the application for this platform, and then restart platform again.                                                                                                                                                                                                                                                                            |
| SUBSEQUENT ACTION | If necessary, reboot host machine this platform is located on. Then reinstall and restart all applications on this machine. If faulty state is a commonly occurring event, then the operating system (OS) or hardware may be a problem. Contact Cisco TAC for assistance. It may also be helpful to gather information event/alarm reports that were issued before and after this alarm report. |

Refer to the [“Obtaining Technical Assistance” section on page xxxviii](#) for detailed instructions on contacting Cisco TAC and opening a service request.

## MAINTENANCE (7)

To troubleshoot and correct the cause of the alarm, refer to the [“Mate Rejected Changeover - Maintenance \(7\)” section on page 7-78](#).

|                   |                                                                                                                                                                                                                                                                                                                                                                             |
|-------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| DESCRIPTION       | Keep Alive Module: Mate Rejected Changeover (KAM: Mate Rejected Changeover)                                                                                                                                                                                                                                                                                                 |
| SEVERITY          | MAJOR                                                                                                                                                                                                                                                                                                                                                                       |
| THRESHOLD         | 100                                                                                                                                                                                                                                                                                                                                                                         |
| THROTTLE          | 0                                                                                                                                                                                                                                                                                                                                                                           |
| DATAWORDS         | Local State - STRING [30]<br>Mate State - STRING [30]                                                                                                                                                                                                                                                                                                                       |
| PRIMARY CAUSE     | Mate is not yet in stable state.                                                                                                                                                                                                                                                                                                                                            |
| PRIMARY ACTION    | Enter the status command to get information on the two systems in the pair (primary and secondary Element Management System (EMS), Call Agent (CA) or Feature Server (FS)).                                                                                                                                                                                                 |
| SECONDARY CAUSE   | Mate detects itself faulty during changeover and then rejects changeover.<br><b>Note</b> This attempted changeover could be caused by a forced (operator) switch, or could be caused by secondary instance rejecting changeover as primary is being brought up.                                                                                                             |
| SECONDARY ACTION  | If mate is faulty (not running), then perform the corrective action steps listed for the MAINTENANCE (4) event.                                                                                                                                                                                                                                                             |
| TERNARY ACTION    | If both systems (local and mate) are still running, diagnose whether both instances are operating in stable state (one in active and the other in standby). If both are in a stable state, wait 10 minutes and try the “control” command again.                                                                                                                             |
| SUBSEQUENT ACTION | If standby side is not in stable state, bring down the standby side and restart software using the “platform stop” and “platform start” commands. If software restart does not resolve the problem, or if the problem is commonly occurring, contact Cisco TAC. It may be necessary to reinstall software. Additional OS or hardware problems may also need to be resolved. |

Refer to the [“Obtaining Technical Assistance” section on page xxxviii](#) for detailed instructions on contacting Cisco TAC and opening a service request.



## MAINTENANCE (8)

To troubleshoot and correct the cause of the alarm, refer to the [“Mate Changeover Timeout - Maintenance \(8\)”](#) section on page 7-81.

|                   |                                                                                                                                                                                                                                                                      |
|-------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| DESCRIPTION       | Keep Alive Module: Mate Changeover Timeout (KAM: Mate Changeover Timeout)                                                                                                                                                                                            |
| SEVERITY          | MAJOR                                                                                                                                                                                                                                                                |
| THRESHOLD         | 100                                                                                                                                                                                                                                                                  |
| THROTTLE          | 0                                                                                                                                                                                                                                                                    |
| DATAWORDS         | Local State - STRING [30]<br>Mate State - STRING [30]                                                                                                                                                                                                                |
| PRIMARY CAUSE     | Faulty mate.                                                                                                                                                                                                                                                         |
| PRIMARY ACTION    | Review information from CLI log report concerning faulty mate.                                                                                                                                                                                                       |
| SECONDARY ACTION  | This alarm is usually caused by a software problem on the specific mate platform identified in the alarm report.                                                                                                                                                     |
| TERNARY ACTION    | On the mate platform identified in this alarm report, restart the platform.                                                                                                                                                                                          |
| SUBSEQUENT ACTION | If mate platform restart is not successful, reinstall the application for this mate platform, and then restart mate platform again. If necessary, reboot host machine this mate platform is located on. Then reinstall and restart all applications on that machine. |

## MAINTENANCE (9)

To troubleshoot and correct the cause of the alarm, refer to the [“Local Initialization Failure - Maintenance \(9\)”](#) section on page 7-81.

|                  |                                                                                                                       |
|------------------|-----------------------------------------------------------------------------------------------------------------------|
| DESCRIPTION      | Keep Alive Module: Local Initialization Failure (KAM: Local Initialization Failure)                                   |
| SEVERITY         | MAJOR                                                                                                                 |
| THRESHOLD        | 100                                                                                                                   |
| THROTTLE         | 0                                                                                                                     |
| DATAWORDS        | Local State - STRING [30]<br>Mate State - STRING [30]                                                                 |
| PRIMARY CAUSE    | Local initialization has failed.                                                                                      |
| PRIMARY ACTION   | When this event report is issued, the system has failed and the re-initialization process has failed.                 |
| SECONDARY ACTION | Check that the binary files are present for the unit (Call Agent, Feature Server, Element Manager).                   |
| TERNARY ACTION   | If the files are not present, then re-install the files from initial or backup media. Then restart the failed device. |

## MAINTENANCE (10)

To troubleshoot and correct the cause of the alarm, refer to the [“Local Initialization Timeout - Maintenance \(10\)” section on page 7-81](#).

|                  |                                                                                                                       |
|------------------|-----------------------------------------------------------------------------------------------------------------------|
| DESCRIPTION      | Keep Alive Module: Local Initialization Timeout (KAM: Local Initialization Timeout)                                   |
| SEVERITY         | MAJOR                                                                                                                 |
| THRESHOLD        | 100                                                                                                                   |
| THROTTLE         | 0                                                                                                                     |
| DATAWORDS        | Local State - STRING [30]<br>Mate State - STRING [30]                                                                 |
| PRIMARY CAUSE    | Local initialization has timed out.                                                                                   |
| PRIMARY ACTION   | Check that the binary files are present for the unit (Call Agent, Feature Server, or Element Manager).                |
| SECONDARY CAUSE  | When the event report is issued, the system has failed and the re-initialization process has failed.                  |
| SECONDARY ACTION | If the files are not present, then re-install the files from initial or backup media. Then restart the failed device. |

## MAINTENANCE (11)

For additional information, refer to the [“Switchover Complete - Maintenance \(11\)” section on page 7-59](#).

|                |                                                               |
|----------------|---------------------------------------------------------------|
| DESCRIPTION    | Switchover Complete                                           |
| SEVERITY       | INFO                                                          |
| THRESHOLD      | 100                                                           |
| THROTTLE       | 0                                                             |
| DATAWORDS      | Local State - STRING [30]<br>Mate State - STRING [30]         |
| PRIMARY CAUSE  | Acknowledges that the changeover successfully completed.      |
| PRIMARY ACTION | Informational event report and no further action is required. |

## MAINTENANCE (12)

For additional information, refer to the [“Initialization Successful - Maintenance \(12\)”](#) section on page 7-59.

|                |                                                                               |
|----------------|-------------------------------------------------------------------------------|
| DESCRIPTION    | Keep Alive Module: Initialization Successful (KAM: Initialization Successful) |
| SEVERITY       | INFO                                                                          |
| THRESHOLD      | 100                                                                           |
| THROTTLE       | 0                                                                             |
| DATAWORDS      | Local State - STRING [30]<br>Mate State - STRING [30]                         |
| PRIMARY CAUSE  | Initiates a local initialization that is successful.                          |
| PRIMARY ACTION | Informational event report and no further action is required.                 |

## MAINTENANCE (13)

For additional information, refer to the [“Administrative State Change - Maintenance \(13\)”](#) section on page 7-60.

|                |                                                                                                                                                                        |
|----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| DESCRIPTION    | Administrative State Change (Admin State Change)                                                                                                                       |
| SEVERITY       | INFO                                                                                                                                                                   |
| THRESHOLD      | 100                                                                                                                                                                    |
| THROTTLE       | 0                                                                                                                                                                      |
| DATAWORDS      | Facility Type - STRING [40]<br>Facility ID - STRING [40]<br>Initial Admin State - STRING [20]<br>Target Admin State - STRING [20]<br>Current Admin State - STRING [20] |
| PRIMARY CAUSE  | The administrative state of a managed resource has changed.                                                                                                            |
| PRIMARY ACTION | No action is required, since this informational event report is given after manually changing the administrative state of a managed resource.                          |

## MAINTENANCE (14)

For additional information, refer to the [“Call Agent Administrative State Change - Maintenance \(14\)” section on page 7-60.](#)

|                |                                                                                                                      |
|----------------|----------------------------------------------------------------------------------------------------------------------|
| DESCRIPTION    | Call Agent Administrative State Change                                                                               |
| SEVERITY       | INFO                                                                                                                 |
| THRESHOLD      | 100                                                                                                                  |
| THROTTLE       | 0                                                                                                                    |
| DATAWORDS      | Call Agent ID - STRING [40]<br>Current Local State - STRING [40]<br>Current Mate State - STRING [20]                 |
| PRIMARY CAUSE  | Indicates that call agent has changed operational state as a result of a manual switchover (control command in CLI). |
| PRIMARY ACTION | No action is required.                                                                                               |

## MAINTENANCE (15)

For additional information, refer to the [“Feature Server Administrative State Change - Maintenance \(15\)” section on page 7-60.](#)

|                |                                                                                                                                               |
|----------------|-----------------------------------------------------------------------------------------------------------------------------------------------|
| DESCRIPTION    | Feature Server Administrative State Change                                                                                                    |
| SEVERITY       | INFO                                                                                                                                          |
| THRESHOLD      | 100                                                                                                                                           |
| THROTTLE       | 0                                                                                                                                             |
| DATAWORDS      | Feature Server ID - STRING [40]<br>Feature Server Type - STRING [40]<br>Current Local State - STRING [20]<br>Current Mate State - STRING [20] |
| PRIMARY CAUSE  | Indicates that call agent has changed operational state as a result of a manual switchover (control command in CLI).                          |
| PRIMARY ACTION | No action is required.                                                                                                                        |

## MAINTENANCE (16)

For additional information, refer to the [“Process Manager: Starting Process - Maintenance \(16\)”](#) section on page 7-60.

|                |                                                                                                                    |
|----------------|--------------------------------------------------------------------------------------------------------------------|
| DESCRIPTION    | Process Manager: Starting Process (PMG: Starting Process)                                                          |
| SEVERITY       | INFO                                                                                                               |
| THRESHOLD      | 100                                                                                                                |
| THROTTLE       | 0                                                                                                                  |
| DATAWORDS      | Process Name - STRING [40]<br>Restart Type - STRING [40]<br>Restart Mode - STRING [32]<br>Process Group - ONE_BYTE |
| PRIMARY CAUSE  | Process is being started as system is being brought up.                                                            |
| PRIMARY ACTION | No action is required.                                                                                             |

## MAINTENANCE (17)

For additional information, refer to the [“Invalid Event Report Received - Maintenance \(17\)”](#) section on page 7-60.

|                  |                                                                                                                                                                                      |
|------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| DESCRIPTION      | Invalid Event Report Received                                                                                                                                                        |
| SEVERITY         | INFO                                                                                                                                                                                 |
| THRESHOLD        | 100                                                                                                                                                                                  |
| THROTTLE         | 0                                                                                                                                                                                    |
| DATAWORDS        | Report Type - TWO_BYTES<br>Report Number - TWO_BYTES<br>Validation Failure - STRING [30]                                                                                             |
| PRIMARY CAUSE    | Indicates that a process has sent an event report that cannot be found in the database.                                                                                              |
| PRIMARY ACTION   | If during system initialization a short burst of these event reports are issued prior to the database initialization, then these event reports are informational and can be ignored. |
| SECONDARY ACTION | Otherwise, contact Cisco TAC technical support for more information. (Contact Cisco TAC.)                                                                                            |

Refer to the [“Obtaining Technical Assistance”](#) section on page xxxviii for detailed instructions on contacting Cisco TAC and opening a service request.

## MAINTENANCE (18)

To troubleshoot and correct the cause of the alarm, refer to the [“Process Manager: Process has Died - Maintenance \(18\)” section on page 7-81](#).

|                |                                                                                |
|----------------|--------------------------------------------------------------------------------|
| DESCRIPTION    | Process Manager: Process has Died (PMG: Process has Died)                      |
| SEVERITY       | MINOR                                                                          |
| THRESHOLD      | 100                                                                            |
| THROTTLE       | 0                                                                              |
| DATAWORDS      | Process Name - STRING [40]<br>Process Group - FOUR_BYTES                       |
| PRIMARY CAUSE  | This alarm is caused by a software problem.                                    |
| PRIMARY ACTION | If problem persists, contact Cisco TAC technical support. (Contact Cisco TAC.) |

Refer to the [“Obtaining Technical Assistance” section on page xxxviii](#) for detailed instructions on contacting Cisco TAC and opening a service request.

## MAINTENANCE (19)

To troubleshoot and correct the cause of the alarm, refer to the [“Process Manager: Process Exceeded Restart Rate - Maintenance \(19\)” section on page 7-81](#).

|                   |                                                                                                                                                                                    |
|-------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| DESCRIPTION       | Process Manager: Process Exceeded Restart Rate (PMG: Process Exceeded Restart Rate)                                                                                                |
| SEVERITY          | MAJOR                                                                                                                                                                              |
| THRESHOLD         | 100                                                                                                                                                                                |
| THROTTLE          | 0                                                                                                                                                                                  |
| DATAWORDS         | Process Name - STRING [40]<br>Restart Rate - FOUR_BYTES<br>Process Group - ONE_BYTE                                                                                                |
| PRIMARY CAUSE     | This alarm is usually caused by a software problem on the specific platform identified in the alarm report. Soon after this event is issued, one platform will go to faulty state. |
| PRIMARY ACTION    | Review information from CLI log report.                                                                                                                                            |
| SECONDARY ACTION  | On the platform identified in this alarm report, restart the platform.                                                                                                             |
| TERNARY ACTION    | If platform restart is not successful, reinstall the application for this platform, and then restart platform again.                                                               |
| SUBSEQUENT ACTION | If necessary, reboot host machine this platform is located on. Then reinstall and restart all applications on this machine.                                                        |

## MAINTENANCE (20)

To troubleshoot and correct the cause of the alarm, refer to the [“Lost Connection to Mate - Maintenance \(20\)” section on page 7-82](#).

|                  |                                                                                                         |
|------------------|---------------------------------------------------------------------------------------------------------|
| DESCRIPTION      | Keep Alive Module: Lost Connection to Mate (KAM: Lost KAM Connection to Mate)                           |
| SEVERITY         | MAJOR                                                                                                   |
| THRESHOLD        | 100                                                                                                     |
| THROTTLE         | 0                                                                                                       |
| DATAWORDS        | Mate Ping - STRING [50]                                                                                 |
| PRIMARY CAUSE    | Network interface hardware problem.                                                                     |
| PRIMARY ACTION   | Check whether the network interface is down. If so, restore network interface and restart the software. |
| SECONDARY CAUSE  | The alarm can be caused by a router problem.                                                            |
| SECONDARY ACTION | If router problem, then repair router and reinstall.                                                    |
| TERNARY CAUSE    | Soon after this event is issued, one platform may go to faulty state.                                   |

## MAINTENANCE (21)

To troubleshoot and correct the cause of the alarm, refer to the [“Network Interface Down - Maintenance \(21\)” section on page 7-82](#).

|                  |                                                                                                         |
|------------------|---------------------------------------------------------------------------------------------------------|
| DESCRIPTION      | Keep Alive Module: Network Interface Down (KAM: Network Interface Down)                                 |
| SEVERITY         | MAJOR                                                                                                   |
| THRESHOLD        | 100                                                                                                     |
| THROTTLE         | 0                                                                                                       |
| DATAWORDS        | IP Address - STRING [50]                                                                                |
| PRIMARY CAUSE    | The alarm is caused by a network interface hardware problem.                                            |
| PRIMARY ACTION   | Subsequently system goes faulty.                                                                        |
| SECONDARY CAUSE  | Soon after this event is issued, one platform may go to faulty state.                                   |
| SECONDARY ACTION | Check whether the network interface is down. If so, restore network interface and restart the software. |

## MAINTENANCE (22)

For additional information, refer to the [“Mate is Alive - Maintenance \(22\)”](#) section on page 7-61.

|             |                                                       |
|-------------|-------------------------------------------------------|
| DESCRIPTION | Keep Alive Module: Mate is Alive (KAM: Mate is Alive) |
| SEVERITY    | INFO                                                  |
| THRESHOLD   | 100                                                   |
| THROTTLE    | 0                                                     |
| DATAWORDS   | Local State - STRING [30]<br>Mate State - STRING [30] |

## MAINTENANCE (23)

To troubleshoot and correct the cause of the alarm, refer to the [“Process Manager: Process Failed to Complete Initialization - Maintenance \(23\)”](#) section on page 7-82.

|                |                                                                                                             |
|----------------|-------------------------------------------------------------------------------------------------------------|
| DESCRIPTION    | Process Manager: Process Failed to Complete Initialization (PMG: Process Failed to Complete Initialization) |
| SEVERITY       | MAJOR                                                                                                       |
| THRESHOLD      | 100                                                                                                         |
| THROTTLE       | 0                                                                                                           |
| DATAWORDS      | Process Name - STRING [40]<br>Process Group - ONE_BYTE                                                      |
| PRIMARY CAUSE  | The specified process failed to complete initialization during the restoral process.                        |
| PRIMARY ACTION | Verify that the specified process’s binary image is installed. If not, install it and restart the platform. |



## MAINTENANCE (24)

To troubleshoot and correct the cause of the alarm, refer to the [“Process Manager: Restarting Process - Maintenance \(24\)”](#) section on page 7-82.

|                |                                                                                                                    |
|----------------|--------------------------------------------------------------------------------------------------------------------|
| DESCRIPTION    | Process Manager: Restarting Process (PMG: Restarting Process)                                                      |
| SEVERITY       | MINOR                                                                                                              |
| THRESHOLD      | 100                                                                                                                |
| THROTTLE       | 0                                                                                                                  |
| DATAWORDS      | Process Name - STRING [40]<br>Restart Type - STRING [40]<br>Restart Mode - STRING [32]<br>Process Group - ONE_BYTE |
| PRIMARY CAUSE  | Software problem process has exited abnormally and had to be restarted.                                            |
| PRIMARY ACTION | If problem persists, contact Cisco TAC.                                                                            |

Refer to the [“Obtaining Technical Assistance”](#) section on page xxxviii for detailed instructions on contacting Cisco TAC and opening a service request.

## MAINTENANCE (25)

For additional information, refer to the [“Process Manager: Changing State - Maintenance \(25\)”](#) section on page 7-61.

|             |                                                       |
|-------------|-------------------------------------------------------|
| DESCRIPTION | Process Manager: Changing State (PMG: Changing State) |
| SEVERITY    | INFO                                                  |
| THRESHOLD   | 100                                                   |
| THROTTLE    | 0                                                     |
| DATAWORDS   | Platform State - STRING [40]                          |

## MAINTENANCE (26)

To troubleshoot and correct the cause of the alarm, refer to the [“Process Manager: Going Faulty - Maintenance \(26\)” section on page 7-82.](#)

|                |                                                                                                                                                                                                                                                  |
|----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| DESCRIPTION    | Process Manager: Going Faulty (PMG: Going Faulty)                                                                                                                                                                                                |
| SEVERITY       | MAJOR                                                                                                                                                                                                                                            |
| THRESHOLD      | 100                                                                                                                                                                                                                                              |
| THROTTLE       | 0                                                                                                                                                                                                                                                |
| DATAWORDS      | Reason - STRING [40]                                                                                                                                                                                                                             |
| PRIMARY CAUSE  | System has been brought down. The system has detected a fault.                                                                                                                                                                                   |
| PRIMARY ACTION | If it is not due to the operator intentionally bringing down the system, then the platform has detected a fault and has shut down. This is typically followed by MAINTENANCE (3). Use corrective action procedures provided for MAINTENANCE (3). |

## MAINTENANCE (27)

For additional information, refer to the [“Process Manager: Changing Over to Active - Maintenance \(27\)” section on page 7-62.](#)

|             |                                                                         |
|-------------|-------------------------------------------------------------------------|
| DESCRIPTION | Process Manager: Changing Over to Active (PMG: Changing Over to Active) |
| SEVERITY    | INFO                                                                    |
| THRESHOLD   | 100                                                                     |
| THROTTLE    | 0                                                                       |

## MAINTENANCE (28)

For additional information, refer to the [“Process Manager: Changing Over to Standby - Maintenance \(28\)” section on page 7-62.](#)

|             |                                                                           |
|-------------|---------------------------------------------------------------------------|
| DESCRIPTION | Process Manager: Changing Over to Standby (PMG: Changing Over to Standby) |
| SEVERITY    | INFO                                                                      |
| THRESHOLD   | 100                                                                       |
| THROTTLE    | 0                                                                         |

## MAINTENANCE (29)

To monitor and correct the cause of the event, refer to the [“Administrative State Change Failure - Maintenance \(29\)”](#) section on page 7-62.

|                  |                                                                                                                                                                                                                |
|------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| DESCRIPTION      | Administrative State Change Failure (Admin State Change Failure)                                                                                                                                               |
| SEVERITY         | WARNING                                                                                                                                                                                                        |
| THRESHOLD        | 100                                                                                                                                                                                                            |
| THROTTLE         | 0                                                                                                                                                                                                              |
| DATAWORDS        | Facility Type - STRING [40]<br>Facility Instance - STRING [40]<br>Failure Reason - STRING [40]<br>Initial Admin State - STRING [20]<br>Target Admin State - STRING [20]<br>Current Admin State - STRING [20]   |
| PRIMARY CAUSE    | An attempt to change the administrative state of a device has failed.                                                                                                                                          |
| PRIMARY ACTION   | Monitor the system to see if any event reports indicate a database update failure.                                                                                                                             |
| SECONDARY ACTION | If one is found, analyze the cause of the failure. Verify that the controlling element of the targeted device was in the ACTIVE state in order to service the request to change the ADMIN state of the device. |
| TERNARY ACTION   | If the controlling platform instance is not ACTIVE, restore it to service.                                                                                                                                     |

## MAINTENANCE (30)

For additional information, refer to the [“Element Manager State Change - Maintenance \(30\)”](#) section on page 7-62.

|                  |                                                                                                           |
|------------------|-----------------------------------------------------------------------------------------------------------|
| DESCRIPTION      | Element Manager State Change                                                                              |
| SEVERITY         | INFO                                                                                                      |
| THRESHOLD        | 100                                                                                                       |
| THROTTLE         | 0                                                                                                         |
| DATAWORDS        | Element Manager ID - STRING [40]<br>Current Local State - STRING [40]<br>Current Mate State - STRING [40] |
| PRIMARY CAUSE    | The specified EMS has changed to the indicated state either naturally or via user request.                |
| PRIMARY ACTION   | No action is necessary. This is part of the normal state transitioning process for the EMS.               |
| SECONDARY ACTION | Monitor the system for related event reports if the transition was to a faulty or out of service state.   |

**Note**

MAINTENANCE (31) is not used.

## MAINTENANCE (32)

For additional information, refer to the [“Process Manager: Sending Go Active to Process - Maintenance \(32\)” section on page 7-62.](#)

|                |                                                                                                             |
|----------------|-------------------------------------------------------------------------------------------------------------|
| DESCRIPTION    | Process Manager: Sending Go Active to Process (PMG: Sending Go Active to Process)                           |
| SEVERITY       | INFO                                                                                                        |
| THRESHOLD      | 100                                                                                                         |
| THROTTLE       | 0                                                                                                           |
| DATAWORDS      | Process Name - STRING [40]<br>Process Group - ONE_BYTE                                                      |
| PRIMARY CAUSE  | Process is being notified to switch to active state as the system is switching over from standby to active. |
| PRIMARY ACTION | No action is necessary.                                                                                     |

## MAINTENANCE (33)

For additional information, refer to the [“Process Manager: Sending Go Standby to Process - Maintenance \(33\)” section on page 7-62.](#)

|                |                                                                                                                                                                                                                                                                                                   |
|----------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| DESCRIPTION    | Process Manager: Sending Go Standby to Process (PMG: Sending Go Standby to Process)                                                                                                                                                                                                               |
| SEVERITY       | INFO                                                                                                                                                                                                                                                                                              |
| THRESHOLD      | 100                                                                                                                                                                                                                                                                                               |
| THROTTLE       | 0                                                                                                                                                                                                                                                                                                 |
| DATAWORDS      | Process Name - STRING [40]<br>Process Group - ONE_BYTE                                                                                                                                                                                                                                            |
| PRIMARY CAUSE  | Process is being notified to exit gracefully as the system is switching over to standby state, or is shutting down. The switchover or shutdown could be due to either of the following: (1) Operator is taking the action to switch or shut down the system. (2) The system has detected a fault. |
| PRIMARY ACTION | No action is necessary.                                                                                                                                                                                                                                                                           |

## MAINTENANCE (34)

For additional information, refer to the [“Process Manager: Sending End Process to Process - Maintenance \(34\)”](#) section on page 7-63.

|                |                                                                                                                                                                                                                                                                                                   |
|----------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| DESCRIPTION    | Process Manager: Sending End Process to Process (PMG: Sending End Process to Process)                                                                                                                                                                                                             |
| SEVERITY       | INFO                                                                                                                                                                                                                                                                                              |
| THRESHOLD      | 100                                                                                                                                                                                                                                                                                               |
| THROTTLE       | 0                                                                                                                                                                                                                                                                                                 |
| DATAWORDS      | Process Name - STRING [40]<br>Process Group - ONE_BYTE                                                                                                                                                                                                                                            |
| PRIMARY CAUSE  | Process is being notified to exit gracefully as the system is switching over to standby state, or is shutting down. The switchover or shutdown could be due to either of the following: (1) Operator is taking the action to switch or shut down the system. (2) The system has detected a fault. |
| PRIMARY ACTION | No action is necessary.                                                                                                                                                                                                                                                                           |

## MAINTENANCE (35)

For additional information, refer to the [“Process Manager: All Processes Completed Initialization - Maintenance \(35\)”](#) section on page 7-63.

|                |                                                                                                       |
|----------------|-------------------------------------------------------------------------------------------------------|
| DESCRIPTION    | Process Manager: All Processes Completed Initialization (PMG: All Processes Completed Initialization) |
| SEVERITY       | INFO                                                                                                  |
| THRESHOLD      | 100                                                                                                   |
| THROTTLE       | 0                                                                                                     |
| PRIMARY CAUSE  | The system is being brought up, and all processes are ready to start executing.                       |
| PRIMARY ACTION | No action is necessary.                                                                               |

## MAINTENANCE (36)

For additional information, refer to the [“Process Manager: Sending All Processes Initialization Complete to Process - Maintenance \(36\)”](#) section on page 7-63.

|                |                                                                                                                       |
|----------------|-----------------------------------------------------------------------------------------------------------------------|
| DESCRIPTION    | Process Manager: Sending All Processes Init Complete to Process (PMG: Sending All Processes Init Complete to Process) |
| SEVERITY       | INFO                                                                                                                  |
| THRESHOLD      | 100                                                                                                                   |
| THROTTLE       | 0                                                                                                                     |
| DATAWORDS      | Process Name - STRING [40]<br>Process Group - ONE_BYTE                                                                |
| PRIMARY CAUSE  | The system is being brought up, and all processes are being notified to start executing.                              |
| PRIMARY ACTION | No action is necessary.                                                                                               |

## MAINTENANCE (37)

For additional information, refer to the [“Process Manager: Killing Process - Maintenance \(37\)”](#) section on page 7-63.

|                 |                                                                                                       |
|-----------------|-------------------------------------------------------------------------------------------------------|
| DESCRIPTION     | Process Manager: Killing Process (PMG: Killing Process)                                               |
| SEVERITY        | INFO                                                                                                  |
| THRESHOLD       | 100                                                                                                   |
| THROTTLE        | 0                                                                                                     |
| DATAWORDS       | Process Name - STRING [40]<br>Process Group - ONE_BYTE                                                |
| PRIMARY CAUSE   | One of the following software problems occurred while the system was being brought up or shut down.   |
| PRIMARY ACTION  | No action is necessary.                                                                               |
| SECONDARY CAUSE | A process did not come up when the system was brought up and had to be killed in order to restart it. |
| TERNARY CAUSE   | A process did not exit when asked to exit.                                                            |

## MAINTENANCE (38)

For additional information, refer to the [“Process Manager: Clearing the Database - Maintenance \(38\)” section on page 7-63.](#)

|                |                                                                                                                    |
|----------------|--------------------------------------------------------------------------------------------------------------------|
| DESCRIPTION    | Process Manager: Clearing the Database (PMG: Clearing the Database)                                                |
| SEVERITY       | INFO                                                                                                               |
| THRESHOLD      | 100                                                                                                                |
| THROTTLE       | 0                                                                                                                  |
| PRIMARY CAUSE  | The system is preparing to copy data from the mate. (The system has been brought up and the mate side is running.) |
| PRIMARY ACTION | No action is necessary.                                                                                            |

## MAINTENANCE (39)

For additional information, refer to the [“Process Manager: Cleared the Database - Maintenance \(39\)” section on page 7-63.](#)

|                |                                                                                                                   |
|----------------|-------------------------------------------------------------------------------------------------------------------|
| DESCRIPTION    | Process Manager: Cleared the Database (PMG: Cleared the Database)                                                 |
| SEVERITY       | INFO                                                                                                              |
| THRESHOLD      | 100                                                                                                               |
| THROTTLE       | 0                                                                                                                 |
| PRIMARY CAUSE  | The system is prepared to copy data from the mate. (The system has been brought up and the mate side is running.) |
| PRIMARY ACTION | No action is necessary.                                                                                           |

## MAINTENANCE (40)

To troubleshoot and correct the cause of the alarm, refer to the [“Process Manager: Binary Does not Exist for Process - Maintenance \(40\)” section on page 7-82.](#)

|                |                                                                                             |
|----------------|---------------------------------------------------------------------------------------------|
| DESCRIPTION    | Process Manager: Binary Does not Exist for Process (PMG: Binary Does not Exist for Process) |
| SEVERITY       | CRITICAL                                                                                    |
| THRESHOLD      | 100                                                                                         |
| THROTTLE       | 0                                                                                           |
| DATAWORDS      | Program Name - STRING [30]<br>Executable Name - STRING [100]                                |
| PRIMARY CAUSE  | Platform is not installed correctly.                                                        |
| PRIMARY ACTION | Reinstall platform.                                                                         |

## MAINTENANCE (41)

To monitor and correct the cause of the event, refer to the [“Administrative State Change Successful with Warning - Maintenance \(41\)”](#) section on page 7-64.

|                |                                                                                                                                                                                            |
|----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| DESCRIPTION    | Administrative State Change Successful with Warning (Admin State Change Successful with Warning)                                                                                           |
| SEVERITY       | WARNING                                                                                                                                                                                    |
| THRESHOLD      | 100                                                                                                                                                                                        |
| THROTTLE       | 0                                                                                                                                                                                          |
| DATAWORDS      | Facility Type - STRING [40]<br>Facility Instance - STRING [40]<br>Initial State - STRING [20]<br>Target State - STRING [20]<br>Current State - STRING [20]<br>Warning Reason - STRING [40] |
| PRIMARY CAUSE  | Device was in a flux state.                                                                                                                                                                |
| PRIMARY ACTION | Retry command.                                                                                                                                                                             |

## MAINTENANCE (42)

To troubleshoot and correct the cause of the alarm, refer to the [“Number of Heartbeat Messages Received is Less Than 50% of Expected - Maintenance \(42\)”](#) section on page 7-83.

|                |                                                                                                                                                     |
|----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------|
| DESCRIPTION    | Keep Alive Module: Number of Heartbeat Messages Received is Less Than 50% of Expected (KAM: # of HB Messages Received is Less Than 50% of Expected) |
| SEVERITY       | MAJOR                                                                                                                                               |
| THRESHOLD      | 100                                                                                                                                                 |
| THROTTLE       | 0                                                                                                                                                   |
| DATAWORDS      | Interface Name - STRING [50]<br>IP Address - STRING [50]<br>Expected HB Messages - ONE_BYTE<br>HB Messages Received - ONE_BYTE                      |
| PRIMARY CAUSE  | The alarm is caused by a network problem.                                                                                                           |
| PRIMARY ACTION | Fix the network problem.                                                                                                                            |



## MAINTENANCE (43)

To troubleshoot and correct the cause of the alarm, refer to the [“Process Manager: Process Failed to Come Up in Active Mode - Maintenance \(43\)”](#) section on page 7-83.

|                |                                                                                                           |
|----------------|-----------------------------------------------------------------------------------------------------------|
| DESCRIPTION    | Process Manager: Process Failed to Come Up in Active Mode (PMG: Process Failed to Come Up in Active Mode) |
| SEVERITY       | CRITICAL                                                                                                  |
| THRESHOLD      | 100                                                                                                       |
| THROTTLE       | 0                                                                                                         |
| DATAWORDS      | Process Name - STRING [40]<br>Process Group - ONE_BYTE                                                    |
| PRIMARY CAUSE  | The alarm is caused by a software or configuration problem.                                               |
| PRIMARY ACTION | Restart the platform. If problem persists call tech support. (Contact Cisco TAC.)                         |

Refer to the [“Obtaining Technical Assistance”](#) section on page xxxviii for detailed instructions on contacting Cisco TAC and opening a service request.

## MAINTENANCE (44)

To troubleshoot and correct the cause of the alarm, refer to the [“Process Manager: Process Failed to Come Up in Standby Mode - Maintenance \(44\)”](#) section on page 7-83.

|                |                                                                                                             |
|----------------|-------------------------------------------------------------------------------------------------------------|
| DESCRIPTION    | Process Manager: Process Failed to Come Up in Standby Mode (PMG: Process Failed to Come Up in Standby Mode) |
| SEVERITY       | CRITICAL                                                                                                    |
| THRESHOLD      | 100                                                                                                         |
| THROTTLE       | 0                                                                                                           |
| DATAWORDS      | Process Name - STRING [40]<br>Process Group - ONE_BYTE                                                      |
| PRIMARY CAUSE  | The alarm is caused by a software or configuration problem.                                                 |
| PRIMARY ACTION | Restart the platform. If problem persists call tech support. (Contact Cisco TAC.)                           |

Refer to the [“Obtaining Technical Assistance”](#) section on page xxxviii for detailed instructions on contacting Cisco TAC and opening a service request.

## MAINTENANCE (45)

To troubleshoot and correct the cause of the alarm, refer to the [“Application Instance State Change Failure - Maintenance \(45\)”](#) section on page 7-83.

|                |                                                                                     |
|----------------|-------------------------------------------------------------------------------------|
| DESCRIPTION    | Application Instance State Change Failure                                           |
| SEVERITY       | MAJOR                                                                               |
| THRESHOLD      | 100                                                                                 |
| THROTTLE       | 0                                                                                   |
| DATAWORDS      | Application Instance - STRING [20]<br>Failure Reason - STRING [80]                  |
| PRIMARY CAUSE  | Switchover of application instance failed because of a platform fault.              |
| PRIMARY ACTION | Retry switchover and if condition continues call tech support. (Contact Cisco TAC.) |

Refer to the [“Obtaining Technical Assistance”](#) section on page xxxviii for detailed instructions on contacting Cisco TAC and opening a service request.

## MAINTENANCE (46)

For additional information, refer to the [“Network Interface Restored - Maintenance \(46\)”](#) section on page 7-65.

|                |                                                                               |
|----------------|-------------------------------------------------------------------------------|
| DESCRIPTION    | Network Interface Restored                                                    |
| SEVERITY       | INFO                                                                          |
| THRESHOLD      | 100                                                                           |
| THROTTLE       | 0                                                                             |
| DATAWORDS      | Interface Name - STRING [80]<br>Interface IP Address - STRING [80]            |
| PRIMARY CAUSE  | Interface cable is put back and interface is put “up” using ifconfig command. |
| PRIMARY ACTION | No action is required.                                                        |

## MAINTENANCE (47)

To troubleshoot and correct the cause of the alarm, refer to the [“Thread Watchdog Counter Expired for a Thread - Maintenance \(47\)”](#) section on page 7-83.

|                |                                                                                       |
|----------------|---------------------------------------------------------------------------------------|
| DESCRIPTION    | Thread Watchdog Counter Expired for a Thread                                          |
| SEVERITY       | CRITICAL                                                                              |
| THRESHOLD      | 100                                                                                   |
| THROTTLE       | 0                                                                                     |
| DATAWORDS      | Process Name - STRING [5]<br>Thread Type - FOUR_BYTES<br>Thread Instance - FOUR_BYTES |
| PRIMARY CAUSE  | The alarm is caused by a software error.                                              |
| PRIMARY ACTION | No action is required. (The system will automatically recover or shutdown.)           |

## MAINTENANCE (48)

To troubleshoot and correct the cause of the alarm, refer to the [“Index Table Usage Exceeded Minor Usage Threshold Level - Maintenance \(48\)”](#) section on page 7-84.

|                  |                                                                                                               |
|------------------|---------------------------------------------------------------------------------------------------------------|
| DESCRIPTION      | Index Table Usage Exceeded Minor Usage Threshold Level (IDX Table Usage Exceeded Minor Usage Threshold Level) |
| SEVERITY         | MINOR                                                                                                         |
| THRESHOLD        | 100                                                                                                           |
| THROTTLE         | 0                                                                                                             |
| DATAWORDS        | Table Name - STRING [80]<br>Size - FOUR_BYTES<br>Used - FOUR_BYTES                                            |
| PRIMARY CAUSE    | Call traffic is above design limits.                                                                          |
| PRIMARY ACTION   | Verify that traffic is within rated capacity.                                                                 |
| SECONDARY CAUSE  | Software problem requiring manufacture analysis.                                                              |
| SECONDARY ACTION | Contact customer support. (Contact Cisco TAC.)                                                                |

Refer to the [“Obtaining Technical Assistance”](#) section on page xxxviii for detailed instructions on contacting Cisco TAC and opening a service request.

## MAINTENANCE (49)

To troubleshoot and correct the cause of the alarm, refer to the [“Index Table Usage Exceeded Major Usage Threshold Level - Maintenance \(49\)”](#) section on page 7-84.

|                  |                                                                                                               |
|------------------|---------------------------------------------------------------------------------------------------------------|
| DESCRIPTION      | Index Table Usage Exceeded Major Usage Threshold Level (IDX Table Usage Exceeded Major Usage Threshold Level) |
| SEVERITY         | MAJOR                                                                                                         |
| THRESHOLD        | 100                                                                                                           |
| THROTTLE         | 0                                                                                                             |
| DATAWORDS        | Table Name - STRING [80]<br>Table Size - FOUR_BYTES<br>Used - FOUR_BYTES                                      |
| PRIMARY CAUSE    | Call traffic is above design limits.                                                                          |
| PRIMARY ACTION   | Verify that traffic is within rated capacity.                                                                 |
| SECONDARY CAUSE  | Software problem requiring manufacture analysis has occurred.                                                 |
| SECONDARY ACTION | Contact customer support. (Contact Cisco TAC.)                                                                |

Refer to the [“Obtaining Technical Assistance”](#) section on page xxxviii for detailed instructions on contacting Cisco TAC and opening a service request.

## MAINTENANCE (50)

To troubleshoot and correct the cause of the alarm, refer to the [“Index Table Usage Exceeded Critical Usage Threshold Level - Maintenance \(50\)”](#) section on page 7-84.

|                  |                                                                                                                     |
|------------------|---------------------------------------------------------------------------------------------------------------------|
| DESCRIPTION      | Index Table Usage Exceeded Critical Usage Threshold Level (IDX Table Usage Exceeded Critical Usage Threshold Level) |
| SEVERITY         | CRITICAL                                                                                                            |
| THRESHOLD        | 100                                                                                                                 |
| THROTTLE         | 0                                                                                                                   |
| DATAWORDS        | Table Name - STRING [80]<br>Table Size - FOUR_BYTES<br>Used - FOUR_BYTES                                            |
| PRIMARY CAUSE    | Call traffic is above design limits.                                                                                |
| PRIMARY ACTION   | Verify that traffic is within rated capacity.                                                                       |
| SECONDARY CAUSE  | Software problem requiring manufacture analysis has occurred.                                                       |
| SECONDARY ACTION | Contact customer support. (Contact Cisco TAC.)                                                                      |

## MAINTENANCE (51)

To troubleshoot and correct the cause of the alarm, refer to the [“A Process Exceeds 70% of Central Processing Unit Usage - Maintenance \(51\)”](#) section on page 7-84.

|                |                                                                                                       |
|----------------|-------------------------------------------------------------------------------------------------------|
| DESCRIPTION    | A Process Exceeds 70% of Central Processing Unit Usage (A Process Exceeds 70% of CPU Usage)           |
| SEVERITY       | MAJOR                                                                                                 |
| THRESHOLD      | 100                                                                                                   |
| THROTTLE       | 0                                                                                                     |
| DATAWORDS      | Host Name - STRING [40]<br>PID - STRING [40]<br>Process Name - STRING [40]<br>CPU Usage - STRING [40] |
| PRIMARY CAUSE  | A process has entered a state of erratic behavior.                                                    |
| PRIMARY ACTION | Monitor the process and kill it if necessary.                                                         |

## MAINTENANCE (52)

For additional information, refer to the [“Central Processing Unit Usage is Now Below the 50% Level - Maintenance \(52\)”](#) section on page 7-66.

|                |                                                                                                       |
|----------------|-------------------------------------------------------------------------------------------------------|
| DESCRIPTION    | Central Processing Unit Usage is Now Below the 50% Level (CPU Usage is Now Below the 50% Level)       |
| SEVERITY       | INFO                                                                                                  |
| THRESHOLD      | 100                                                                                                   |
| THROTTLE       | 0                                                                                                     |
| DATAWORDS      | Host Name - STRING [40]<br>PID - STRING [40]<br>Process Name - STRING [40]<br>CPU Usage - STRING [40] |
| PRIMARY CAUSE  | No probable cause is necessary.                                                                       |
| PRIMARY ACTION | No corrective action is necessary.                                                                    |

## MAINTENANCE (53)

To troubleshoot and correct the cause of the alarm, refer to the [“The Central Processing Unit Usage is Over 90% Busy - Maintenance \(53\)”](#) section on page 7-84.

|                |                                                                                     |
|----------------|-------------------------------------------------------------------------------------|
| DESCRIPTION    | The Central Processing Unit Usage is Over 90% Busy (The CPU Usage is Over 90% Busy) |
| SEVERITY       | CRITICAL                                                                            |
| THRESHOLD      | 100                                                                                 |
| THROTTLE       | 0                                                                                   |
| DATAWORDS      | Host Name - STRING [40]<br>CPU Usage - STRING [40]                                  |
| PRIMARY CAUSE  | To numerous to determine.                                                           |
| PRIMARY ACTION | Try to isolate the problem. Call Cisco for assistance. (Contact Cisco TAC.)         |

Refer to the [“Obtaining Technical Assistance”](#) section on page xxxviii for detailed instructions on contacting Cisco TAC and opening a service request.

## MAINTENANCE (54)

For additional information, refer to the [“The Central Processing Unit has Returned to Normal Levels of Operation - Maintenance \(54\)”](#) section on page 7-66.

|                |                                                                                                                             |
|----------------|-----------------------------------------------------------------------------------------------------------------------------|
| DESCRIPTION    | The Central Processing Unit has Returned to Normal Levels of Operation (The CPU has Returned to Normal Levels of Operation) |
| SEVERITY       | INFO                                                                                                                        |
| THRESHOLD      | 100                                                                                                                         |
| THROTTLE       | 0                                                                                                                           |
| DATAWORDS      | Host Name - STRING [40]<br>CPU Usage - STRING [40]                                                                          |
| PRIMARY CAUSE  | N/A                                                                                                                         |
| PRIMARY ACTION | N/A                                                                                                                         |

## MAINTENANCE (55)

To troubleshoot and correct the cause of the alarm, refer to the [“The Five Minute Load Average is Abnormally High - Maintenance \(55\)”](#) section on page 7-85.

|                |                                                                                                                                                                                                                                                                                          |
|----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| DESCRIPTION    | The Five Minute Load Average is Abnormally High                                                                                                                                                                                                                                          |
| SEVERITY       | MAJOR                                                                                                                                                                                                                                                                                    |
| THRESHOLD      | 100                                                                                                                                                                                                                                                                                      |
| THROTTLE       | 0                                                                                                                                                                                                                                                                                        |
| DATAWORDS      | Host Name - STRING [40]<br>Load Average - STRING [40]                                                                                                                                                                                                                                    |
| PRIMARY CAUSE  | Multiple processes are vying for processing time on the system, which is normal in a high traffic situation such as heavy call processing or bulk provisioning.                                                                                                                          |
| PRIMARY ACTION | Monitor the system to ensure all subsystems are performing normally. If so, only lightening the effective load on the system will clear the situation. If not, verify which process(es) are running at abnormally high rates, provide the information to Cisco TAC. (Contact Cisco TAC.) |

Refer to the [“Obtaining Technical Assistance”](#) section on page xxxviii for detailed instructions on contacting Cisco TAC and opening a service request.

## MAINTENANCE (56)

For additional information, refer to the [“The Load Average has Returned to Normal Levels - Maintenance \(56\)”](#) section on page 7-66.

|                |                                                       |
|----------------|-------------------------------------------------------|
| DESCRIPTION    | The Load Average has Returned to Normal Levels        |
| SEVERITY       | INFO                                                  |
| THRESHOLD      | 100                                                   |
| THROTTLE       | 0                                                     |
| DATAWORDS      | Host Name - STRING [40]<br>Load Average - STRING [40] |
| PRIMARY CAUSE  | N/A                                                   |
| PRIMARY ACTION | N/A                                                   |

## MAINTENANCE (57)

To troubleshoot and correct the cause of the alarm, refer to the [“Memory and Swap are Consumed at Critical Levels - Maintenance \(57\)”](#) section on page 7-85.



### Note

Maintenance (57) is issued by the BTS 10200 system when memory consumption is greater than 95 percent (>95%) and swap space consumption is greater than 50 percent (>50%).

|                |                                                                                                                                                                                                                                                                                          |
|----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| DESCRIPTION    | Memory and Swap are Consumed at Critical Levels                                                                                                                                                                                                                                          |
| SEVERITY       | CRITICAL                                                                                                                                                                                                                                                                                 |
| THRESHOLD      | 100                                                                                                                                                                                                                                                                                      |
| THROTTLE       | 0                                                                                                                                                                                                                                                                                        |
| DATAWORDS      | Host Name - STRING [40]<br>Memory - STRING [40]<br>Swap - STRING [40]                                                                                                                                                                                                                    |
| PRIMARY CAUSE  | A process or multiple processes have consumed a critical amount of memory on the system and the operating system is utilizing a critical amount of the swap space for process execution. This can be a result of high call rates or bulk provisioning activity.                          |
| PRIMARY ACTION | Monitor the system to ensure all subsystems are performing normally. If so, only lightening the effective load on the system will clear the situation. If not, verify which process(es) are running at abnormally high rates, provide the information to Cisco TAC. (Contact Cisco TAC.) |

Refer to the [“Obtaining Technical Assistance”](#) section on page xxxviii for detailed instructions on contacting Cisco TAC and opening a service request.



## MAINTENANCE (58)

For additional information, refer to the [“Memory and Swap are Consumed at Abnormal Levels - Maintenance \(58\)”](#) section on page 7-67.


**Note**

Maintenance (58) is issued by the BTS 10200 system when memory consumption is greater than 80 percent (>80%) and swap space consumption is greater than 30 percent (>30%).

|                |                                                                                                                                                                                                                                                                                          |
|----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| DESCRIPTION    | Memory and Swap are Consumed at Abnormal Levels                                                                                                                                                                                                                                          |
| SEVERITY       | INFO                                                                                                                                                                                                                                                                                     |
| THRESHOLD      | 100                                                                                                                                                                                                                                                                                      |
| THROTTLE       | 0                                                                                                                                                                                                                                                                                        |
| DATAWORDS      | Host Name - STRING [40]<br>Memory - STRING [40]<br>Swap - STRING [40]                                                                                                                                                                                                                    |
| PRIMARY CAUSE  | A process or multiple processes have consumed an abnormal amount of memory on the system and the operating system is utilizing an abnormal amount of the swap space for process execution. This can be a result of high call rates or bulk provisioning activity.                        |
| PRIMARY ACTION | Monitor the system to ensure all subsystems are performing normally. If so, only lightening the effective load on the system will clear the situation. If not, verify which process(es) are running at abnormally high rates, provide the information to Cisco TAC. (Contact Cisco TAC.) |

Refer to the [“Obtaining Technical Assistance”](#) section on page xxxviii for detailed instructions on contacting Cisco TAC and opening a service request.


**Note**

MAINTENANCE (59) and MAINTENANCE (60) are not used.

## MAINTENANCE (61)

To troubleshoot and correct the cause of the alarm, refer to the [“No Heartbeat Messages Received Through the Interface - Maintenance \(61\)”](#) section on page 7-85.

|                  |                                                                                                      |
|------------------|------------------------------------------------------------------------------------------------------|
| DESCRIPTION      | No Heartbeat Messages Received Through the Interface (No HB Messages Received Through the Interface) |
| SEVERITY         | CRITICAL                                                                                             |
| THRESHOLD        | 100                                                                                                  |
| THROTTLE         | 0                                                                                                    |
| DATAWORDS        | Interface Name - STRING [20]<br>Interface IP Address - STRING [50]                                   |
| PRIMARY CAUSE    | Local network interface is down.                                                                     |
| PRIMARY ACTION   | Restore the local network interface.                                                                 |
| SECONDARY CAUSE  | Mate network interface on the same sub-net is faulty.                                                |
| SECONDARY ACTION | Restore mate network interface.                                                                      |
| TERNARY CAUSE    | Network congestion.                                                                                  |

## MAINTENANCE (62)

To troubleshoot and correct the cause of the alarm, refer to the [“Link Monitor: Interface Lost Communication - Maintenance \(62\)”](#) section on page 7-85.

|                 |                                                                                      |
|-----------------|--------------------------------------------------------------------------------------|
| DESCRIPTION     | Link Monitor: Interface Lost Communication                                           |
| SEVERITY        | MAJOR                                                                                |
| THRESHOLD       | 100                                                                                  |
| THROTTLE        | 0                                                                                    |
| DATAWORDS       | Interface Name - STRING [80]<br>Interface IP Address - STRING [80]                   |
| PRIMARY CAUSE   | Interface cable is pulled out or the interface is set “down” using ifconfig command. |
| PRIMARY ACTION  | Restore the network interface.                                                       |
| SECONDARY CAUSE | Interface has no connectivity to any of the machines or routers.                     |

## MAINTENANCE (63)

To troubleshoot and correct the cause of the alarm, refer to the [“Outgoing Heartbeat Period Exceeded Limit - Maintenance \(63\)”](#) section on page 7-86.

|                |                                                                                                                                                                                               |
|----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| DESCRIPTION    | Outgoing Heartbeat Period Exceeded Limit                                                                                                                                                      |
| SEVERITY       | MAJOR                                                                                                                                                                                         |
| THRESHOLD      | 100                                                                                                                                                                                           |
| THROTTLE       | 0                                                                                                                                                                                             |
| DATAWORDS      | Max. HB Period (ms) - FOUR_BYTES<br>HB Period (ms) - FOUR_BYTES                                                                                                                               |
| PRIMARY CAUSE  | This is caused by system performance degradation due to central processing unit (CPU) overload or excessive I/O operations.                                                                   |
| PRIMARY ACTION | Identify the applications which are causing the system degradation via CLI commands to verify if this is a persistent or on-going situation. Contact Cisco TAC with the gathered information. |

Refer to the [“Obtaining Technical Assistance”](#) section on page xxxviii for detailed instructions on contacting Cisco TAC and opening a service request.

## MAINTENANCE (64)

To troubleshoot and correct the cause of the alarm, refer to the [“Average Outgoing Heartbeat Period Exceeds Major Alarm Limit - Maintenance \(64\)”](#) section on page 7-86.

|                |                                                                                                                                                                                               |
|----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| DESCRIPTION    | Average Outgoing Heartbeat Period Exceeds Major Alarm Limit (Average Outgoing HB Period Exceeds Maj Alarm Limit)                                                                              |
| SEVERITY       | MAJOR                                                                                                                                                                                         |
| THRESHOLD      | 100                                                                                                                                                                                           |
| THROTTLE       | 0                                                                                                                                                                                             |
| DATAWORDS      | Max. Avg HB Period - FOUR_BYTES<br>Avg. HB Period (ms) - FOUR_BYTES                                                                                                                           |
| PRIMARY CAUSE  | This is caused by system performance degradation due to CPU overload or excessive I/O operations.                                                                                             |
| PRIMARY ACTION | Identify the applications which are causing the system degradation via CLI commands to verify if this is a persistent or on-going situation. Contact Cisco TAC with the gathered information. |

Refer to the [“Obtaining Technical Assistance”](#) section on page xxxviii for detailed instructions on contacting Cisco TAC and opening a service request.

## MAINTENANCE (65)

To troubleshoot and correct the cause of the alarm, refer to the [“Disk Partition Critically Consumed - Maintenance \(65\)” section on page 7-86](#).

|                |                                                                                 |
|----------------|---------------------------------------------------------------------------------|
| DESCRIPTION    | Disk Partition Critically Consumed                                              |
| SEVERITY       | CRITICAL                                                                        |
| THRESHOLD      | 100                                                                             |
| THROTTLE       | 0                                                                               |
| DATAWORDS      | Directory - STRING [32]<br>Device - STRING [32]<br>Percentage Used - STRING [8] |
| PRIMARY CAUSE  | A process or processes is/are writing extraneous data to the named partition.   |
| PRIMARY ACTION | Perform disk clean-up and maintenance on the offending system.                  |

## MAINTENANCE (66)

To troubleshoot and correct the cause of the alarm, refer to the [“Disk Partition Significantly Consumed - Maintenance \(66\)” section on page 7-86](#).

|                |                                                                                 |
|----------------|---------------------------------------------------------------------------------|
| DESCRIPTION    | Disk Partition Significantly Consumed                                           |
| SEVERITY       | MAJOR                                                                           |
| THRESHOLD      | 100                                                                             |
| THROTTLE       | 0                                                                               |
| DATAWORDS      | Directory - STRING [32]<br>Device - STRING [32]<br>Percentage Used - STRING [8] |
| PRIMARY CAUSE  | A process or processes is/are writing extraneous data to the named partition.   |
| PRIMARY ACTION | Perform disk clean-up and maintenance on the offending system.                  |

## MAINTENANCE (67)

To troubleshoot and correct the cause of the alarm, refer to the [“The Free Inter-Process Communication Pool Buffers Below Minor Threshold - Maintenance \(67\)”](#) section on page 7-86.

|                |                                                                                                                                                     |
|----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------|
| DESCRIPTION    | The Free Inter-Process Communication Pool Buffers Below Minor Threshold (The Free IPC Pool Buffers Below Minor Threshold)                           |
| SEVERITY       | MINOR                                                                                                                                               |
| THRESHOLD      | 100                                                                                                                                                 |
| THROTTLE       | 0                                                                                                                                                   |
| DATAWORDS      | Free IPC Pool Buffer - STRING [10]<br>Threshold - STRING [10]                                                                                       |
| PRIMARY CAUSE  | IPC pool buffers are not being freed properly by the application or the application is not able to keep up with the incoming IPC messaging traffic. |
| PRIMARY ACTION | Contact Cisco TAC immediately.                                                                                                                      |

Refer to the [“Obtaining Technical Assistance”](#) section on page xxxviii for detailed instructions on contacting Cisco TAC and opening a service request.

## MAINTENANCE (68)

To troubleshoot and correct the cause of the alarm, refer to the [“The Free Inter-Process Communication Pool Buffers Below Major Threshold - Maintenance \(68\)”](#) section on page 7-87.

|                |                                                                                                                                                                                   |
|----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| DESCRIPTION    | The Free Inter-Process Communication Pool Buffers Below Major Threshold (The Free IPC Pool Buffers Below Major Threshold)                                                         |
| SEVERITY       | MAJOR                                                                                                                                                                             |
| THRESHOLD      | 100                                                                                                                                                                               |
| THROTTLE       | 0                                                                                                                                                                                 |
| DATAWORDS      | Free IPC Poll Buffer - STRING [10]<br>Threshold - STRING [10]                                                                                                                     |
| PRIMARY CAUSE  | Inter-process communication (IPC) pool buffers are not being freed properly by the application or the application is not able to keep up with the incoming IPC messaging traffic. |
| PRIMARY ACTION | Contact Cisco TAC immediately.                                                                                                                                                    |

Refer to the [“Obtaining Technical Assistance”](#) section on page xxxviii for detailed instructions on contacting Cisco TAC and opening a service request.

## MAINTENANCE (69)

To troubleshoot and correct the cause of the alarm, refer to the [“The Free Inter-Process Communication Pool Buffers Below Critical Threshold - Maintenance \(69\)”](#) section on page 7-87.

|                |                                                                                                                                                     |
|----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------|
| DESCRIPTION    | The Free Inter-Process Communication Pool Buffers Below Critical Threshold (The Free IPC Pool Buffers Below Critical Threshold)                     |
| SEVERITY       | CRITICAL                                                                                                                                            |
| THRESHOLD      | 100                                                                                                                                                 |
| THROTTLE       | 0                                                                                                                                                   |
| DATAWORDS      | Free IPC Poll Buffer - STRING [10]<br>Threshold - STRING [10]                                                                                       |
| PRIMARY CAUSE  | IPC pool buffers are not being freed properly by the application or the application is not able to keep up with the incoming IPC messaging traffic. |
| PRIMARY ACTION | Contact Cisco TAC immediately.                                                                                                                      |

Refer to the [“Obtaining Technical Assistance”](#) section on page xxxviii for detailed instructions on contacting Cisco TAC and opening a service request.

## MAINTENANCE (70)

To troubleshoot and correct the cause of the alarm, refer to the [“The Free Inter-Process Communication Pool Buffer Count Below Minimum Required - Maintenance \(70\)”](#) section on page 7-87.

|                |                                                                                                                                                     |
|----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------|
| DESCRIPTION    | The Free Inter-Process Communication Pool Buffer Count Below Minimum Required (The Free IPC Pool Buffer Count Below Minimum Required)               |
| SEVERITY       | CRITICAL                                                                                                                                            |
| THRESHOLD      | 100                                                                                                                                                 |
| THROTTLE       | 0                                                                                                                                                   |
| DATAWORDS      | Free IPC Buffer Coun - TWO_BYTES<br>Minimum Count - TWO_BYTES                                                                                       |
| PRIMARY CAUSE  | IPC pool buffers are not being freed properly by the application or the application is not able to keep up with the incoming IPC messaging traffic. |
| PRIMARY ACTION | Contact Cisco TAC immediately.                                                                                                                      |

Refer to the [“Obtaining Technical Assistance”](#) section on page xxxviii for detailed instructions on contacting Cisco TAC and opening a service request.

## MAINTENANCE (71)

To troubleshoot and correct the cause of the alarm, refer to the [“Local Domain Name System Server Response Too Slow - Maintenance \(71\)”](#) section on page 7-87.

|                |                                                                                        |
|----------------|----------------------------------------------------------------------------------------|
| DESCRIPTION    | Local Domain Name System Server Response Too Slow (Local DNS Server Response Too Slow) |
| SEVERITY       | MAJOR                                                                                  |
| THRESHOLD      | 100                                                                                    |
| THROTTLE       | 0                                                                                      |
| DATAWORDS      | DNS Server IP - STRING [64]                                                            |
| PRIMARY CAUSE  | Local domain name system (DNS) server too busy.                                        |
| PRIMARY ACTION | Check the local DNS server.                                                            |

## MAINTENANCE (72)

To troubleshoot and correct the cause of the alarm, refer to the [“External Domain Name System Server Response Too Slow - Maintenance \(72\)”](#) section on page 7-87.

|                 |                                                                                                                                                                                                                                      |
|-----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| DESCRIPTION     | External Domain Name System Server Response Too Slow (External DNS Server Response Too Slow)                                                                                                                                         |
| SEVERITY        | MAJOR                                                                                                                                                                                                                                |
| THRESHOLD       | 100                                                                                                                                                                                                                                  |
| THROTTLE        | 0                                                                                                                                                                                                                                    |
| DATAWORDS       | DNS Server IP - STRING [64]                                                                                                                                                                                                          |
| PRIMARY CAUSE   | The network traffic is busy, or the nameserver is very busy.                                                                                                                                                                         |
| PRIMARY ACTION  | Check the DNS server(s).                                                                                                                                                                                                             |
| SECONDARY CAUSE | There is an daemon called monitorDNS.sh checking DNS server every minute or so. It will issue alarm if it cannot contact the DNS server or the response is slow. But it will clear the alarm if later it can contact the DNS server. |

## MAINTENANCE (73)

To troubleshoot and correct the cause of the alarm, refer to the [“External Domain Name System Server not Responsive - Maintenance \(73\)”](#) section on page 7-88.

|                 |                                                                                                                                                                                                                                      |
|-----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| DESCRIPTION     | External Domain Name System Server not Responsive (External DNS Server not Responsive)                                                                                                                                               |
| SEVERITY        | CRITICAL                                                                                                                                                                                                                             |
| THRESHOLD       | 100                                                                                                                                                                                                                                  |
| THROTTLE        | 0                                                                                                                                                                                                                                    |
| DATAWORDS       | DNS Server IP - STRING [64]                                                                                                                                                                                                          |
| PRIMARY CAUSE   | DNS servers or the network may be down.                                                                                                                                                                                              |
| PRIMARY ACTION  | Check the DNS server(s).                                                                                                                                                                                                             |
| SECONDARY CAUSE | There is an daemon called monitorDNS.sh checking DNS server every minute or so. It will issue alarm if it cannot contact the DNS server or the response is slow. But it will clear the alarm if later it can contact the DNS server. |

## MAINTENANCE (74)

To troubleshoot and correct the cause of the alarm, refer to the [“Local Domain Name System Service not Responsive - Maintenance \(74\)”](#) section on page 7-88.

|                |                                                                                    |
|----------------|------------------------------------------------------------------------------------|
| DESCRIPTION    | Local Domain Name System Service not Responsive (Local DNS Service not Responsive) |
| SEVERITY       | CRITICAL                                                                           |
| THRESHOLD      | 100                                                                                |
| THROTTLE       | 0                                                                                  |
| DATAWORDS      | DNS Server IP - STRING [64]                                                        |
| PRIMARY CAUSE  | Local DNS service may be down.                                                     |
| PRIMARY ACTION | Check the local DNS server.                                                        |



## MAINTENANCE (75)

To monitor and correct the cause of the event, refer to the [“Mismatch of Internet Protocol Address Local Server and Domain Name System - Maintenance \(75\)”](#) section on page 7-70.

|                |                                                                                                                                                                        |
|----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| DESCRIPTION    | Mismatch of Internet Protocol Address Local Server and Domain Name System (Mismatch of IP Addr % Local Server and DNS)                                                 |
| SEVERITY       | WARNING                                                                                                                                                                |
| THRESHOLD      | 100                                                                                                                                                                    |
| THROTTLE       | 0                                                                                                                                                                      |
| DATAWORDS      | Host Name - STRING [64]<br>IP Addr Local Server - STRING [64]<br>IP Addr DNS Server - STRING [64]                                                                      |
| PRIMARY CAUSE  | DNS updates are not getting to the Cisco BTS 10200 Softswitch from the external server, or the discrepancy was detected before the local DNS lookup table was updated. |
| PRIMARY ACTION | Ensure the external DNS server is operational and sending updates to the Cisco BTS 10200 Softswitch.                                                                   |



### Note

MAINTENANCE (76) is not used.

## MAINTENANCE (77)

To troubleshoot and correct the cause of the alarm, refer to the [“Mate Time Differs Beyond Tolerance - Maintenance \(77\)”](#) section on page 7-88.

|                |                                                                               |
|----------------|-------------------------------------------------------------------------------|
| DESCRIPTION    | Mate Time Differs Beyond Tolerance                                            |
| SEVERITY       | MAJOR                                                                         |
| THRESHOLD      | 100                                                                           |
| THROTTLE       | 0                                                                             |
| DATAWORDS      | Max Time Difference - FOUR_BYTES<br>Actual Time Difference - FOUR_BYTES       |
| PRIMARY CAUSE  | Time synchronization is not working.                                          |
| PRIMARY ACTION | Change UNIX time on the Faulty/Standby side. If Standby, stop platform first. |

## MAINTENANCE (78)

For additional information, refer to the [“Bulk Data Management System Admin State Change - Maintenance \(78\)” section on page 7-70.](#)

|                |                                                                                             |
|----------------|---------------------------------------------------------------------------------------------|
| DESCRIPTION    | Bulk Data Management System Admin State Change (BDMS Admin State Change)                    |
| SEVERITY       | INFO                                                                                        |
| THRESHOLD      | 100                                                                                         |
| THROTTLE       | 0                                                                                           |
| DATAWORDS      | Application Instance - STRING [40]<br>Local State - STRING [40]<br>Mate State - STRING [40] |
| PRIMARY CAUSE  | The Bulk Data Management Server (BDMS) was switched over manually.                          |
| PRIMARY ACTION | None                                                                                        |

## MAINTENANCE (79)

For additional information, refer to the [“Resource Reset - Maintenance \(79\)” section on page 7-70.](#)

|                |                                                                |
|----------------|----------------------------------------------------------------|
| DESCRIPTION    | Resource Reset                                                 |
| SEVERITY       | INFO                                                           |
| THRESHOLD      | 100                                                            |
| THROTTLE       | 0                                                              |
| DATAWORDS      | Resource Type - STRING [40]<br>Resource Instance - STRING [40] |
| PRIMARY CAUSE  | Trunk-Termination<br>Subscriber-Termination<br>Media Gateways  |
| PRIMARY ACTION | None                                                           |

## MAINTENANCE (80)

For additional information, refer to the [“Resource Reset Warning - Maintenance \(80\)”](#) section on page 7-70.

|                |                                                                                                 |
|----------------|-------------------------------------------------------------------------------------------------|
| DESCRIPTION    | Resource Reset Warning                                                                          |
| SEVERITY       | INFO                                                                                            |
| THRESHOLD      | 100                                                                                             |
| THROTTLE       | 0                                                                                               |
| DATAWORDS      | Resource Type - STRING [40]<br>Resource Instance - STRING [40]<br>Warning Reason - STRING [120] |
| PRIMARY CAUSE  | Trunk-Termination<br>Subscriber-Termination<br>Media Gateway                                    |
| PRIMARY ACTION | None                                                                                            |

## MAINTENANCE (81)

For additional information, refer to the [“Resource Reset Failure - Maintenance \(81\)”](#) section on page 7-70.

|                |                                                                                                                                                                                   |
|----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| DESCRIPTION    | Resource Reset Failure                                                                                                                                                            |
| SEVERITY       | INFO                                                                                                                                                                              |
| THRESHOLD      | 100                                                                                                                                                                               |
| THROTTLE       | 0                                                                                                                                                                                 |
| DATAWORDS      | Resource Type - STRING [40]<br>Resource Instance - STRING [40]<br>Failure Reason - STRING [120]                                                                                   |
| PRIMARY CAUSE  | This the result of an internal messaging error.                                                                                                                                   |
| PRIMARY ACTION | Check Dataword 3 (Failure Reason) to determine if this is caused by invalid user input, inconsistent provisioning of the device, or if the system is busy and a timeout occurred. |

## MAINTENANCE (82)

To troubleshoot and correct the cause of the alarm, refer to the [“Average Outgoing Heartbeat Period Exceeds Critical Limit - Maintenance \(82\)”](#) section on page 7-88.

|                |                                                                                                              |
|----------------|--------------------------------------------------------------------------------------------------------------|
| DESCRIPTION    | Average Outgoing Heartbeat Period Exceeds Critical Limit (Average Outgoing HB Period Exceeds Critical Limit) |
| SEVERITY       | CRITICAL                                                                                                     |
| THRESHOLD      | 100                                                                                                          |
| THROTTLE       | 0                                                                                                            |
| DATAWORDS      | Critical Threshold F - FOUR_BYTES<br>Current Average HB Peri - FOUR_BYTES                                    |
| PRIMARY CAUSE  | CPU is overloaded.                                                                                           |
| PRIMARY ACTION | Shutdown platform.                                                                                           |

## MAINTENANCE (83)

To troubleshoot and correct the cause of the alarm, refer to the [“Swap Space Below Minor Threshold - Maintenance \(83\)”](#) section on page 7-88.

|                  |                                                                      |
|------------------|----------------------------------------------------------------------|
| DESCRIPTION      | Swap Space Below Minor Threshold                                     |
| SEVERITY         | MINOR                                                                |
| THRESHOLD        | 5                                                                    |
| THROTTLE         | 0                                                                    |
| DATAWORDS        | Minor Threshold (MB) - FOUR_BYTES<br>Current Value (MB) - FOUR_BYTES |
| PRIMARY CAUSE    | Too many processes are running.                                      |
| PRIMARY ACTION   | Stop proliferation of executables (processes-scripts).               |
| SECONDARY CAUSE  | File spaces /tmp or /var/run are over-used.                          |
| SECONDARY ACTION | Cleanup file systems.                                                |

## MAINTENANCE (84)

To troubleshoot and correct the cause of the alarm, refer to the [“Swap Space Below Major Threshold - Maintenance \(84\)” section on page 7-88.](#)

|                  |                                                                      |
|------------------|----------------------------------------------------------------------|
| DESCRIPTION      | Swap Space Below Major Threshold                                     |
| SEVERITY         | MAJOR                                                                |
| THRESHOLD        | 5                                                                    |
| THROTTLE         | 0                                                                    |
| DATAWORDS        | Major Threshold (MB) - FOUR_BYTES<br>Current Value (MB) - FOUR_BYTES |
| PRIMARY CAUSE    | Too many processes are running.                                      |
| PRIMARY ACTION   | Stop proliferation of executables (processes/shell-procedures).      |
| SECONDARY CAUSE  | File spaces /tmp or /var/run are over-used.                          |
| SECONDARY ACTION | Cleanup file systems.                                                |

## MAINTENANCE (85)

To troubleshoot and correct the cause of the alarm, refer to the [“Swap Space Below Critical Threshold - Maintenance \(85\)” section on page 7-89.](#)

|                  |                                                                       |
|------------------|-----------------------------------------------------------------------|
| DESCRIPTION      | Swap Space Below Critical Threshold                                   |
| SEVERITY         | CRITICAL                                                              |
| THRESHOLD        | 5                                                                     |
| THROTTLE         | 0                                                                     |
| DATAWORDS        | Critical Threshold (M - FOUR_BYTES<br>Current Value (MB) - FOUR_BYTES |
| PRIMARY CAUSE    | Too many processes are running.                                       |
| PRIMARY ACTION   | Restart Cisco BTS 10200 Softswitch software or reboot system.         |
| SECONDARY CAUSE  | File spaces /tmp or /var/run are over-used.                           |
| SECONDARY ACTION | Cleanup these file systems.                                           |

## MAINTENANCE (86)

To troubleshoot and correct the cause of the alarm, refer to the [“System Health Report Collection Error - Maintenance \(86\)” section on page 7-89](#).

|                |                                                       |
|----------------|-------------------------------------------------------|
| DESCRIPTION    | System Health Report Collection Error                 |
| SEVERITY       | MINOR                                                 |
| THRESHOLD      | 100                                                   |
| THROTTLE       | 0                                                     |
| DATAWORDS      | ErrString - STRING [64]                               |
| PRIMARY CAUSE  | An error occur while collecting system health report. |
| PRIMARY ACTION | Contact Cisco TAC for support.                        |

Refer to the [“Obtaining Technical Assistance” section on page xxxviii](#) for detailed instructions on contacting Cisco TAC and opening a service request.

## MAINTENANCE (87)

To troubleshoot and correct the cause of the alarm, refer to the [“Status Update Process Request Failed - Maintenance \(87\)” section on page 7-89](#).

|                |                                                         |
|----------------|---------------------------------------------------------|
| DESCRIPTION    | Status Update Process Request Failed                    |
| SEVERITY       | MAJOR                                                   |
| THRESHOLD      | 100                                                     |
| THROTTLE       | 0                                                       |
| DATAWORDS      | ErrString - STRING [64]<br>Component Type - STRING [64] |
| PRIMARY CAUSE  | The “status” command is not working properly.           |
| PRIMARY ACTION | Verify “status” command is working properly via CLI.    |

## MAINTENANCE (88)

To troubleshoot and correct the cause of the alarm, refer to the [“Status Update Process Database List Retrieval Error - Maintenance \(88\)”](#) section on page 7-89.

|                |                                                                                                     |
|----------------|-----------------------------------------------------------------------------------------------------|
| DESCRIPTION    | Status Update Process Database List Retrieval Error (Status Update Process DB List Retrieval Error) |
| SEVERITY       | MAJOR                                                                                               |
| THRESHOLD      | 100                                                                                                 |
| THROTTLE       | 0                                                                                                   |
| DATAWORDS      | ErrString - STRING [64]                                                                             |
| PRIMARY CAUSE  | Oracle database (DB) is not working properly.                                                       |
| PRIMARY ACTION | Contact Cisco TAC for support.                                                                      |

Refer to the [“Obtaining Technical Assistance”](#) section on page xxxviii for detailed instructions on contacting Cisco TAC and opening a service request.

## MAINTENANCE (89)

To troubleshoot and correct the cause of the alarm, refer to the [“Status Update Process Database Update Error - Maintenance \(89\)”](#) section on page 7-89.

|                |                                                                                     |
|----------------|-------------------------------------------------------------------------------------|
| DESCRIPTION    | Status Update Process Database Update Error (Status Update Process DB Update Error) |
| SEVERITY       | MAJOR                                                                               |
| THRESHOLD      | 100                                                                                 |
| THROTTLE       | 0                                                                                   |
| DATAWORDS      | ErrString - STRING [64]<br>SQL Command - STRING [64]                                |
| PRIMARY CAUSE  | MySQL DB on EMS is not working properly.                                            |
| PRIMARY ACTION | Contact Cisco TAC for support.                                                      |

Refer to the [“Obtaining Technical Assistance”](#) section on page xxxviii for detailed instructions on contacting Cisco TAC and opening a service request.

## MAINTENANCE (90)

To troubleshoot and correct the cause of the alarm, refer to the [“Disk Partition Moderately Consumed - Maintenance \(90\)”](#) section on page 7-89.

|                |                                                                                 |
|----------------|---------------------------------------------------------------------------------|
| DESCRIPTION    | Disk Partition Moderately Consumed                                              |
| SEVERITY       | MINOR                                                                           |
| THRESHOLD      | 100                                                                             |
| THROTTLE       | 0                                                                               |
| DATAWORDS      | Directory - STRING [32]<br>Device - STRING [32]<br>Percentage Used - STRING [8] |
| PRIMARY CAUSE  | A process or processes is/are writing extraneous data to the named partition.   |
| PRIMARY ACTION | Perform disk clean-up and maintenance on the offending system.                  |

## MAINTENANCE (91)

To troubleshoot and correct the cause of the alarm, refer to the [“Internet Protocol Manager Configuration File Error - Maintenance \(91\)”](#) section on page 7-90.

|                |                                                                            |
|----------------|----------------------------------------------------------------------------|
| DESCRIPTION    | Internet Protocol Manager Configuration File Error (IPM Config File Error) |
| SEVERITY       | CRITICAL                                                                   |
| THRESHOLD      | 100                                                                        |
| THROTTLE       | 0                                                                          |
| DATAWORDS      | Reason - STRING [128]                                                      |
| PRIMARY CAUSE  | Internet Protocol Manager (IPM) config file error.                         |
| PRIMARY ACTION | Check IPM config file (ipm.cfg) for incorrect syntax.                      |



## MAINTENANCE (92)

To troubleshoot and correct the cause of the alarm, refer to the [“Internet Protocol Manager Initialization Error - Maintenance \(92\)”](#) section on page 7-90.

|                |                                                                           |
|----------------|---------------------------------------------------------------------------|
| DESCRIPTION    | Internet Protocol Manager Initialization Error (IPM Initialization Error) |
| SEVERITY       | MAJOR                                                                     |
| THRESHOLD      | 100                                                                       |
| THROTTLE       | 0                                                                         |
| DATAWORDS      | Reason - STRING [128]                                                     |
| PRIMARY CAUSE  | IPM failed to initialize correctly.                                       |
| PRIMARY ACTION | Check Reason dataword as to cause of error.                               |

## MAINTENANCE (93)

To troubleshoot and correct the cause of the alarm, refer to the [“Internet Protocol Manager Interface Failure - Maintenance \(93\)”](#) section on page 7-90.

|                |                                                                     |
|----------------|---------------------------------------------------------------------|
| DESCRIPTION    | Internet Protocol Manager Interface Failure (IPM Interface Failure) |
| SEVERITY       | MAJOR                                                               |
| THRESHOLD      | 100                                                                 |
| THROTTLE       | 0                                                                   |
| DATAWORDS      | Interface Name - STRING [32]<br>Reason - STRING [128]               |
| PRIMARY CAUSE  | IPM failed to create logical interface.                             |
| PRIMARY ACTION | Check Reason dataword as to cause of error.                         |

## MAINTENANCE (94)

For additional information, refer to the [“Internet Protocol Manager Interface State Change - Maintenance \(94\)” section on page 7-72.](#)

|                |                                                                               |
|----------------|-------------------------------------------------------------------------------|
| DESCRIPTION    | Internet Protocol Manager Interface State Change (IPM Interface State Change) |
| SEVERITY       | INFO                                                                          |
| THRESHOLD      | 100                                                                           |
| THROTTLE       | 0                                                                             |
| DATAWORDS      | Interface Name - STRING [32]<br>State - STRING [16]                           |
| PRIMARY CAUSE  | IPM changed state on an interface (up/down).                                  |
| PRIMARY ACTION | None                                                                          |

## MAINTENANCE (95)

For additional information, refer to the [“Internet Protocol Manager Interface Created - Maintenance \(95\)” section on page 7-73.](#)

|                |                                                                                                                                                                              |
|----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| DESCRIPTION    | Internet Protocol Manager Interface Created (IPM Interface Created)                                                                                                          |
| SEVERITY       | INFO                                                                                                                                                                         |
| THRESHOLD      | 100                                                                                                                                                                          |
| THROTTLE       | 0                                                                                                                                                                            |
| DATAWORDS      | Hostname - STRING [128]<br>Physical IF Name - STRING [32]<br>Logical IF Name - STRING [32]<br>IP Addr - STRING [32]<br>Netmask - STRING [32]<br>Broadcast Addr - STRING [32] |
| PRIMARY CAUSE  | IPM created a new logical interface.                                                                                                                                         |
| PRIMARY ACTION | None                                                                                                                                                                         |

## MAINTENANCE (96)

For additional information, refer to the [“Internet Protocol Manager Interface Removed - Maintenance \(96\)” section on page 7-73](#).

|                |                                                                                   |
|----------------|-----------------------------------------------------------------------------------|
| DESCRIPTION    | Internet Protocol Manager Interface Removed (IPM Interface Removed)               |
| SEVERITY       | INFO                                                                              |
| THRESHOLD      | 100                                                                               |
| THROTTLE       | 0                                                                                 |
| DATAWORDS      | Hostname - STRING [128]<br>Logical IF Name - STRING [32]<br>IP Addr - STRING [32] |
| PRIMARY CAUSE  | IPM removed a logical interface.                                                  |
| PRIMARY ACTION | None                                                                              |

## MAINTENANCE (97)

To troubleshoot and correct the cause of the alarm, refer to the [“Inter-Process Communication Input Queue Entered Throttle State - Maintenance \(97\)” section on page 7-90](#).

|                |                                                                                                                                                                                     |
|----------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| DESCRIPTION    | Inter-Process Communication Input Queue Entered Throttle State (IPC Input Queue Entered Throttle State)                                                                             |
| SEVERITY       | CRITICAL                                                                                                                                                                            |
| THRESHOLD      | 500                                                                                                                                                                                 |
| THROTTLE       | 0                                                                                                                                                                                   |
| DATAWORDS      | Process Name - STRING [10]<br>Thread Type - TWO_BYTES<br>Thread Instance - TWO_BYTES<br>Hi Watermark - FOUR_BYTES<br>Lo Watermark - FOUR_BYTES                                      |
| PRIMARY CAUSE  | The indicated thread is not able to process its IPC input messages fast enough, hence the input queue has grown too large and is using up too much of the IPC memory pool resource. |
| PRIMARY ACTION | Contact Cisco TAC.                                                                                                                                                                  |

Refer to the [“Obtaining Technical Assistance” section on page xxxviii](#) for detailed instructions on contacting Cisco TAC and opening a service request.

## MAINTENANCE (98)

To troubleshoot and correct the cause of the alarm, refer to the [“Inter-Process Communication Input Queue Depth at 25% of Its Hi-Watermark - Maintenance \(98\)”](#) section on page 7-90.

|                |                                                                                                                                                                                                 |
|----------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| DESCRIPTION    | Inter-Process Communication Input Queue Depth at 25% of Its Hi-Watermark (IPC Input Queue Depth At 25% Of Its Hi-Watermark)                                                                     |
| SEVERITY       | MINOR                                                                                                                                                                                           |
| THRESHOLD      | 500                                                                                                                                                                                             |
| THROTTLE       | 0                                                                                                                                                                                               |
| DATAWORDS      | Process Name - STRING [10]<br>Thread Type - TWO_BYTES<br>Thread Instance - TWO_BYTES<br>Hi Watermark - FOUR_BYTES<br>Lo Watermark - FOUR_BYTES                                                  |
| PRIMARY CAUSE  | The indicated thread is not able to process its IPC input messages fast enough, hence the input queue has grown too large and is at 25% of the level at which it will enter the throttle state. |
| PRIMARY ACTION | Contact Cisco TAC.                                                                                                                                                                              |

Refer to the [“Obtaining Technical Assistance”](#) section on page xxxviii for detailed instructions on contacting Cisco TAC and opening a service request.

## MAINTENANCE (99)

To troubleshoot and correct the cause of the alarm, refer to the [“Inter-Process Communication Input Queue Depth at 50% of Its Hi-Watermark - Maintenance \(99\)”](#) section on page 7-91.

|                |                                                                                                                                                                                                 |
|----------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| DESCRIPTION    | Inter-Process Communication Input Queue Depth at 50% of Its Hi-Watermark (IPC Input Queue Depth At 50% Of Its Hi-Watermark)                                                                     |
| SEVERITY       | MAJOR                                                                                                                                                                                           |
| THRESHOLD      | 500                                                                                                                                                                                             |
| THROTTLE       | 0                                                                                                                                                                                               |
| DATAWORDS      | Process Name - STRING [10]<br>Thread Type - TWO_BYTES<br>Thread Instance - TWO_BYTES<br>Hi Watermark - FOUR_BYTES<br>Lo Watermark - FOUR_BYTES                                                  |
| PRIMARY CAUSE  | The indicated thread is not able to process its IPC input messages fast enough, hence the input queue has grown too large and is at 50% of the level at which it will enter the throttle state. |
| PRIMARY ACTION | Contact Cisco TAC.                                                                                                                                                                              |

Refer to the [“Obtaining Technical Assistance”](#) section on page xxxviii for detailed instructions on contacting Cisco TAC and opening a service request.

## MAINTENANCE (100)

To troubleshoot and correct the cause of the alarm, refer to the [“Inter-Process Communication Input Queue Depth at 75% of Its Hi-Watermark - Maintenance \(100\)”](#) section on page 7-91.

|                |                                                                                                                                                                                                 |
|----------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| DESCRIPTION    | Inter-Process Communication Input Queue Depth at 75% of Its Hi-Watermark (IPC Input Queue Depth At 75% Of Its Hi-Watermark)                                                                     |
| SEVERITY       | CRITICAL                                                                                                                                                                                        |
| THRESHOLD      | 500                                                                                                                                                                                             |
| THROTTLE       | 0                                                                                                                                                                                               |
| DATAWORDS      | Process Name - STRING [10]<br>Thread Type - TWO_BYTES<br>Thread Instance - TWO_BYTES<br>Hi Watermark - FOUR_BYTES<br>Lo Watermark - FOUR_BYTES                                                  |
| PRIMARY CAUSE  | The indicated thread is not able to process its IPC input messages fast enough, hence the input queue has grown too large and is at 75% of the level at which it will enter the throttle state. |
| PRIMARY ACTION | Contact Cisco TAC.                                                                                                                                                                              |

Refer to the [“Obtaining Technical Assistance”](#) section on page xxxviii for detailed instructions on contacting Cisco TAC and opening a service request.

## MAINTENANCE (101)

To troubleshoot and correct the cause of the alarm, refer to the [“Switchover in Progress - Maintenance \(101\)”](#) section on page 7-91.

|                |                                                                                                                                                                       |
|----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| DESCRIPTION    | Switchover in Progress                                                                                                                                                |
| SEVERITY       | CRITICAL                                                                                                                                                              |
| THRESHOLD      | 100                                                                                                                                                                   |
| THROTTLE       | 0                                                                                                                                                                     |
| DATAWORDS      | Local State - STRING [15]<br>Mate State - STRING [15]<br>Reason - STRING [30]                                                                                         |
| PRIMARY CAUSE  | This alarm is issued when system switchover either due to manual switchover (via CLI command), failover or automatic switchover.                                      |
| PRIMARY ACTION | No action need to be taken, the alarm is cleared when switchover is complete. The service is temporarily suspended for a short period of time during this transition. |

## MAINTENANCE (102)

To troubleshoot and correct the cause of the alarm, refer to the [“Thread Watchdog Counter Close to Expiry for a Thread - Maintenance \(102\)”](#) section on page 7-91.

|                |                                                                                       |
|----------------|---------------------------------------------------------------------------------------|
| DESCRIPTION    | Thread Watchdog Counter Close to Expiry for a Thread                                  |
| SEVERITY       | CRITICAL                                                                              |
| THRESHOLD      | 100                                                                                   |
| THROTTLE       | 0                                                                                     |
| DATAWORDS      | Process Name - STRING [5]<br>Thread Type - FOUR_BYTES<br>Thread Instance - FOUR_BYTES |
| PRIMARY CAUSE  | Software error has occurred.                                                          |
| PRIMARY ACTION | None, the system will automatically recover or shutdown.                              |

## MAINTENANCE (103)

To troubleshoot and correct the cause of the alarm, refer to the [“Central Processing Unit is Offline - Maintenance \(103\)”](#) section on page 7-91.

|                |                                                      |
|----------------|------------------------------------------------------|
| DESCRIPTION    | Central Processing Unit is Offline (CPU Is Offline)  |
| SEVERITY       | CRITICAL                                             |
| THRESHOLD      | 100                                                  |
| THROTTLE       | 0                                                    |
| DATAWORDS      | Hostname - STRING [20]<br>CPU - ONE_BYTE             |
| PRIMARY CAUSE  | An operator action has caused the CPU to go offline. |
| PRIMARY ACTION | Restore CPU or contact Cisco TAC.                    |

Refer to the [“Obtaining Technical Assistance”](#) section on page xxxviii for detailed instructions on contacting Cisco TAC and opening a service request.

# Monitoring Maintenance Events

This section provides the information needed to monitor and correct Maintenance events. [Table 7-2](#) lists all Maintenance events in numerical order and provides cross reference to each subsection in this section.

**Table 7-2** *Cisco BTS 10200 Softswitch Maintenance Events*

| Event Type      | Event Name                                                                                    | Event Severity |
|-----------------|-----------------------------------------------------------------------------------------------|----------------|
| MAINTENANCE(1)  | <a href="#">Test Report - Maintenance (1)</a>                                                 | INFO           |
| MAINTENANCE(2)  | <a href="#">Report Threshold Exceeded - Maintenance (2)</a>                                   | INFO           |
| MAINTENANCE(3)  | <a href="#">Local Side has Become Faulty - Maintenance (3)</a>                                | MAJOR          |
| MAINTENANCE(4)  | <a href="#">Mate Side has Become Faulty - Maintenance (4)</a>                                 | MAJOR          |
| MAINTENANCE(5)  | <a href="#">Changeover Failure - Maintenance (5)</a>                                          | MAJOR          |
| MAINTENANCE(6)  | <a href="#">Changeover Timeout - Maintenance (6)</a>                                          | MAJOR          |
| MAINTENANCE(7)  | <a href="#">Mate Rejected Changeover - Maintenance (7)</a>                                    | MAJOR          |
| MAINTENANCE(8)  | <a href="#">Mate Changeover Timeout - Maintenance (8)</a>                                     | MAJOR          |
| MAINTENANCE(9)  | <a href="#">Local Initialization Failure - Maintenance (9)</a>                                | MAJOR          |
| MAINTENANCE(10) | <a href="#">Local Initialization Timeout - Maintenance (10)</a>                               | MAJOR          |
| MAINTENANCE(11) | <a href="#">Switchover Complete - Maintenance (11)</a>                                        | INFO           |
| MAINTENANCE(12) | <a href="#">Initialization Successful - Maintenance (12)</a>                                  | INFO           |
| MAINTENANCE(13) | <a href="#">Administrative State Change - Maintenance (13)</a>                                | INFO           |
| MAINTENANCE(14) | <a href="#">Call Agent Administrative State Change - Maintenance (14)</a>                     | INFO           |
| MAINTENANCE(15) | <a href="#">Feature Server Administrative State Change - Maintenance (15)</a>                 | INFO           |
| MAINTENANCE(16) | <a href="#">Process Manager: Starting Process - Maintenance (16)</a>                          | INFO           |
| MAINTENANCE(17) | <a href="#">Invalid Event Report Received - Maintenance (17)</a>                              | INFO           |
| MAINTENANCE(18) | <a href="#">Process Manager: Process has Died - Maintenance (18)</a>                          | MINOR          |
| MAINTENANCE(19) | <a href="#">Process Manager: Process Exceeded Restart Rate - Maintenance (19)</a>             | MAJOR          |
| MAINTENANCE(20) | <a href="#">Lost Connection to Mate - Maintenance (20)</a>                                    | MAJOR          |
| MAINTENANCE(21) | <a href="#">Network Interface Down - Maintenance (21)</a>                                     | MAJOR          |
| MAINTENANCE(22) | <a href="#">Mate is Alive - Maintenance (22)</a>                                              | INFO           |
| MAINTENANCE(23) | <a href="#">Process Manager: Process Failed to Complete Initialization - Maintenance (23)</a> | MAJOR          |
| MAINTENANCE(24) | <a href="#">Process Manager: Restarting Process - Maintenance (24)</a>                        | MINOR          |
| MAINTENANCE(25) | <a href="#">Process Manager: Changing State - Maintenance (25)</a>                            | INFO           |
| MAINTENANCE(26) | <a href="#">Process Manager: Going Faulty - Maintenance (26)</a>                              | MAJOR          |
| MAINTENANCE(27) | <a href="#">Process Manager: Changing Over to Active - Maintenance (27)</a>                   | INFO           |
| MAINTENANCE(28) | <a href="#">Process Manager: Changing Over to Standby - Maintenance (28)</a>                  | INFO           |
| MAINTENANCE(29) | <a href="#">Administrative State Change Failure - Maintenance (29)</a>                        | WARNING        |
| MAINTENANCE(30) | <a href="#">Element Manager State Change - Maintenance (30)</a>                               | INFO           |
| MAINTENANCE(32) | <a href="#">Process Manager: Sending Go Active to Process - Maintenance (32)</a>              | INFO           |
| MAINTENANCE(33) | <a href="#">Process Manager: Sending Go Standby to Process - Maintenance (33)</a>             | INFO           |

Table 7-2 Cisco BTS 10200 Softswitch Maintenance Events (continued)

| Event Type      | Event Name                                                                                   | Event Severity |
|-----------------|----------------------------------------------------------------------------------------------|----------------|
| MAINTENANCE(34) | Process Manager: Sending End Process to Process - Maintenance (34)                           | INFO           |
| MAINTENANCE(35) | Process Manager: All Processes Completed Initialization - Maintenance (35)                   | INFO           |
| MAINTENANCE(36) | Process Manager: Sending All Processes Initialization Complete to Process - Maintenance (36) | INFO           |
| MAINTENANCE(37) | Process Manager: Killing Process - Maintenance (37)                                          | INFO           |
| MAINTENANCE(38) | Process Manager: Clearing the Database - Maintenance (38)                                    | INFO           |
| MAINTENANCE(39) | Process Manager: Cleared the Database - Maintenance (39)                                     | INFO           |
| MAINTENANCE(40) | Process Manager: Binary Does not Exist for Process - Maintenance (40)                        | CRITICAL       |
| MAINTENANCE(41) | Administrative State Change Successful with Warning - Maintenance (41)                       | WARNING        |
| MAINTENANCE(42) | Number of Heartbeat Messages Received is Less Than 50% of Expected - Maintenance (42)        | MAJOR          |
| MAINTENANCE(43) | Process Manager: Process Failed to Come Up in Active Mode - Maintenance (43)                 | CRITICAL       |
| MAINTENANCE(44) | Process Manager: Process Failed to Come Up in Standby Mode - Maintenance (44)                | CRITICAL       |
| MAINTENANCE(45) | Application Instance State Change Failure - Maintenance (45)                                 | MAJOR          |
| MAINTENANCE(46) | Network Interface Restored - Maintenance (46)                                                | INFO           |
| MAINTENANCE(47) | Thread Watchdog Counter Expired for a Thread - Maintenance (47)                              | CRITICAL       |
| MAINTENANCE(48) | Index Table Usage Exceeded Minor Usage Threshold Level - Maintenance (48)                    | MINOR          |
| MAINTENANCE(49) | Index Table Usage Exceeded Major Usage Threshold Level - Maintenance (49)                    | MAJOR          |
| MAINTENANCE(50) | Index Table Usage Exceeded Critical Usage Threshold Level - Maintenance (50)                 | CRITICAL       |
| MAINTENANCE(51) | A Process Exceeds 70% of Central Processing Unit Usage - Maintenance (51)                    | MAJOR          |
| MAINTENANCE(52) | Central Processing Unit Usage is Now Below the 50% Level - Maintenance (52)                  | INFO           |
| MAINTENANCE(53) | The Central Processing Unit Usage is Over 90% Busy - Maintenance (53)                        | CRITICAL       |
| MAINTENANCE(54) | The Central Processing Unit has Returned to Normal Levels of Operation - Maintenance (54)    | INFO           |
| MAINTENANCE(55) | The Five Minute Load Average is Abnormally High - Maintenance (55)                           | MAJOR          |
| MAINTENANCE(56) | The Load Average has Returned to Normal Levels - Maintenance (56)                            | INFO           |
| MAINTENANCE(57) | Memory and Swap are Consumed at Critical Levels - Maintenance (57)                           | CRITICAL       |
| MAINTENANCE(58) | Memory and Swap are Consumed at Abnormal Levels - Maintenance (58)                           | INFO           |
| MAINTENANCE(61) | No Heartbeat Messages Received Through the Interface - Maintenance (61)                      | CRITICAL       |
| MAINTENANCE(62) | Link Monitor: Interface Lost Communication - Maintenance (62)                                | MAJOR          |
| MAINTENANCE(63) | Outgoing Heartbeat Period Exceeded Limit - Maintenance (63)                                  | MAJOR          |
| MAINTENANCE(64) | Average Outgoing Heartbeat Period Exceeds Major Alarm Limit - Maintenance (64)               | MAJOR          |
| MAINTENANCE(65) | Disk Partition Critically Consumed - Maintenance (65)                                        | CRITICAL       |
| MAINTENANCE(66) | Disk Partition Significantly Consumed - Maintenance (66)                                     | MAJOR          |
| MAINTENANCE(67) | The Free Inter-Process Communication Pool Buffers Below Minor Threshold - Maintenance (67)   | MINOR          |



**Table 7-2 Cisco BTS 10200 Softswitch Maintenance Events (continued)**

| Event Type      | Event Name                                                                                       | Event Severity |
|-----------------|--------------------------------------------------------------------------------------------------|----------------|
| MAINTENANCE(68) | The Free Inter-Process Communication Pool Buffers Below Major Threshold - Maintenance (68)       | MAJOR          |
| MAINTENANCE(69) | The Free Inter-Process Communication Pool Buffers Below Critical Threshold - Maintenance (69)    | CRITICAL       |
| MAINTENANCE(70) | The Free Inter-Process Communication Pool Buffer Count Below Minimum Required - Maintenance (70) | CRITICAL       |
| MAINTENANCE(71) | Local Domain Name System Server Response Too Slow - Maintenance (71)                             | MAJOR          |
| MAINTENANCE(72) | External Domain Name System Server Response Too Slow - Maintenance (72)                          | MAJOR          |
| MAINTENANCE(73) | External Domain Name System Server not Responsive - Maintenance (73)                             | CRITICAL       |
| MAINTENANCE(74) | Local Domain Name System Service not Responsive - Maintenance (74)                               | CRITICAL       |
| MAINTENANCE(75) | Mismatch of Internet Protocol Address Local Server and Domain Name System - Maintenance (75)     | WARNING        |
| MAINTENANCE(76) | Mate Time Differs Beyond Tolerance - Maintenance (77)                                            | N/A            |
| MAINTENANCE(77) | Mate Time Differs Beyond Tolerance - Maintenance (77)                                            | MAJOR          |
| MAINTENANCE(78) | Bulk Data Management System Admin State Change - Maintenance (78)                                | INFO           |
| MAINTENANCE(79) | Resource Reset - Maintenance (79)                                                                | INFO           |
| MAINTENANCE(80) | Resource Reset Warning - Maintenance (80)                                                        | INFO           |
| MAINTENANCE(81) | Resource Reset Failure - Maintenance (81)                                                        | INFO           |
| MAINTENANCE(82) | Average Outgoing Heartbeat Period Exceeds Critical Limit - Maintenance (82)                      | CRITICAL       |
| MAINTENANCE(83) | Swap Space Below Minor Threshold - Maintenance (83)                                              | MINOR          |
| MAINTENANCE(84) | Swap Space Below Major Threshold - Maintenance (84)                                              | MAJOR          |
| MAINTENANCE(85) | Swap Space Below Critical Threshold - Maintenance (85)                                           | CRITICAL       |
| MAINTENANCE(86) | System Health Report Collection Error - Maintenance (86)                                         | MINOR          |
| MAINTENANCE(87) | Status Update Process Request Failed - Maintenance (87)                                          | MAJOR          |
| MAINTENANCE(88) | Status Update Process Database List Retrieval Error - Maintenance (88)                           | MAJOR          |
| MAINTENANCE(89) | Status Update Process Database Update Error - Maintenance (89)                                   | MAJOR          |
| MAINTENANCE(90) | Disk Partition Moderately Consumed - Maintenance (90)                                            | MINOR          |
| MAINTENANCE(91) | Internet Protocol Manager Configuration File Error - Maintenance (91)                            | CRITICAL       |
| MAINTENANCE(92) | Internet Protocol Manager Initialization Error - Maintenance (92)                                | MAJOR          |
| MAINTENANCE(93) | Internet Protocol Manager Interface Failure - Maintenance (93)                                   | MAJOR          |
| MAINTENANCE(94) | Internet Protocol Manager Interface State Change - Maintenance (94)                              | INFO           |
| MAINTENANCE(95) | Internet Protocol Manager Interface Created - Maintenance (95)                                   | INFO           |
| MAINTENANCE(96) | Internet Protocol Manager Interface Removed - Maintenance (96)                                   | INFO           |
| MAINTENANCE(97) | Inter-Process Communication Input Queue Entered Throttle State - Maintenance (97)                | CRITICAL       |
| MAINTENANCE(98) | Inter-Process Communication Input Queue Depth at 25% of its Hi-Watermark - Maintenance (98)      | MINOR          |

**Table 7-2 Cisco BTS 10200 Softswitch Maintenance Events (continued)**

| Event Type       | Event Name                                                                                                   | Event Severity |
|------------------|--------------------------------------------------------------------------------------------------------------|----------------|
| MAINTENANCE(99)  | <a href="#">Inter-Process Communication Input Queue Depth at 50% of its Hi-Watermark - Maintenance (99)</a>  | MAJOR          |
| MAINTENANCE(100) | <a href="#">Inter-Process Communication Input Queue Depth at 75% of its Hi-Watermark - Maintenance (100)</a> | CRITICAL       |
| MAINTENANCE(101) | <a href="#">Switchover in Progress - Maintenance (101)</a>                                                   | CRITICAL       |
| MAINTENANCE(102) | <a href="#">Thread Watchdog Counter Close to Expiry for a Thread - Maintenance (102)</a>                     | CRITICAL       |
| MAINTENANCE(103) | <a href="#">Central Processing Unit is Offline - Maintenance (103)</a>                                       | CRITICAL       |

## Test Report - Maintenance (1)

The Test Report is for testing the maintenance event category. The event is informational and no further action is required.

## Report Threshold Exceeded - Maintenance (2)

The Report Threshold Exceeded event functions as an informational alert that a report threshold has been exceeded. The primary cause of the event is that the threshold for a given report type and number has been exceeded. No further action is required since this is an information report. The root cause event report - threshold should be investigated to determine if there is a service affecting situation.

## Local Side has Become Faulty - Maintenance (3)

The Local Side has Become Faulty alarm (major) indicates that the local side has become faulty. To troubleshoot and correct the cause of the Local Side has Become Faulty alarm, refer to the [“Local Side has Become Faulty - Maintenance \(3\)”](#) section on page 7-77.

## Mate Side has Become Faulty - Maintenance (4)

The Mate Side has Become Faulty alarm (major) indicates that the mate side has become faulty. To troubleshoot and correct the cause of the Mate Side has Become Faulty alarm, refer to the [“Mate Side has Become Faulty - Maintenance \(4\)”](#) section on page 7-77.

## Changeover Failure - Maintenance (5)

The Changeover Failure alarm (major) indicates that a changeover failed. To troubleshoot and correct the cause of the Changeover Failure alarm, refer to the [“Changeover Failure - Maintenance \(5\)”](#) section on page 7-77.

## Changeover Timeout - Maintenance (6)

The Changeover Timeout alarm (major) indicates that a changeover timed out. To troubleshoot and correct the cause of the Changeover Timeout alarm, refer to the [“Changeover Timeout - Maintenance \(6\)” section on page 7-78](#).

## Mate Rejected Changeover - Maintenance (7)

The Mate Rejected Changeover alarm (major) indicates that the mate rejected the changeover. To troubleshoot and correct the cause of the Mate Rejected Changeover alarm, refer to the [“Mate Rejected Changeover - Maintenance \(7\)” section on page 7-78](#).

## Mate Changeover Timeout - Maintenance (8)

The Mate Changeover Timeout alarm (major) indicates that the mate changeover timed out. To troubleshoot and correct the cause of the Mate Changeover Timeout alarm, refer to the [“Mate Changeover Timeout - Maintenance \(8\)” section on page 7-81](#).

## Local Initialization Failure - Maintenance (9)

The Local Initialization Failure alarm (major) indicates that the local initialization has failed. To troubleshoot and correct the cause of the Local Initialization Failure alarm, refer to the [“Local Initialization Failure - Maintenance \(9\)” section on page 7-81](#).

## Local Initialization Timeout - Maintenance (10)

The Local Initialization Timeout alarm (major) indicates that the local initialization has timed out. To troubleshoot and correct the cause of the Local Initialization Timeout alarm, refer to the [“Local Initialization Timeout - Maintenance \(10\)” section on page 7-81](#).

## Switchover Complete - Maintenance (11)

The Switchover Complete event functions as an informational alert that the switchover has been completed. The Switchover Complete event acknowledges that the changeover successfully completed. The event is informational and no further action is required.

## Initialization Successful - Maintenance (12)

The Initialization Successful event functions as an informational alert that the initialization was successful. The Initialization Successful event indicates that a local initialization has been successful. The event is informational and no further action is required.

## Administrative State Change - Maintenance (13)

The Administrative State Change event functions as an informational alert that the administrative state of a managed resource has changed. No action is required, since this informational event is given after manually changing the administrative state of a managed resource.

## Call Agent Administrative State Change - Maintenance (14)

The Call Agent Administrative State Change event functions as an informational alert that indicates that the call agent has changed operational state as a result of a manual switchover. The event is informational and no further action is required.

## Feature Server Administrative State Change - Maintenance (15)

The Feature Server Administrative State Change event functions as an informational alert that indicates that the feature server has changed operational state as a result of a manual switchover. The event is informational and no further action is required.

## Process Manager: Starting Process - Maintenance (16)

The Process Manager: Process has Died: Starting Process event functions as an information alert that indicates that a process is being started as system is being brought up. The event is informational and no further action is required.

## Invalid Event Report Received - Maintenance (17)

The Invalid Event Report Received event functions as an informational alert that indicates that a process has sent an event report that cannot be found in the database. If during system initialization a short burst of these events are issued prior to the database initialization, then these events are informational and can be ignored; otherwise, contact Cisco TAC. Refer to the [“Obtaining Technical Assistance” section on page xxxviii](#) for detailed instructions on contacting Cisco TAC and opening a service request.

## Process Manager: Process has Died - Maintenance (18)

The Process Manager: Process has Died alarm (minor) indicates that a process has died. To troubleshoot and correct the cause of the Process Manager: Process has Died alarm, refer to the [“Process Manager: Process has Died - Maintenance \(18\)” section on page 7-81](#).

## Process Manager: Process Exceeded Restart Rate - Maintenance (19)

The Process Manager: Process Exceeded Restart Rate alarm (major) indicates that a process has exceeded the restart rate. To troubleshoot and correct the cause of the Process Manager: Process Exceeded Restart Rate alarm, refer to the [“Process Manager: Process Exceeded Restart Rate - Maintenance \(19\)” section on page 7-81](#).

## Lost Connection to Mate - Maintenance (20)

The Lost Connection to Mate alarm (major) indicates that the keepalive module connection to the mate has been lost. To troubleshoot and correct the cause of the Lost Connection to Mate alarm, refer to the [“Lost Connection to Mate - Maintenance \(20\)” section on page 7-82](#).

## Network Interface Down - Maintenance (21)

The Network Interface Down alarm (major) indicates that the network interface has gone down. To troubleshoot and correct the cause of the Network Interface Down alarm, refer to the [“Network Interface Down - Maintenance \(21\)” section on page 7-82](#).

## Mate is Alive - Maintenance (22)

The Mate is Alive event functions as an informational alert that the mate is alive. The reporting CA/FS/EMS/BDMS is indicating that its mate has been successfully restored to service. The event is informational and no further action is required.

## Process Manager: Process Failed to Complete Initialization - Maintenance (23)

The Process Manager: Process Failed to Complete Initialization alarm (major) indicates that a PMG process failed to complete initialization. To trouble and correct the cause of the Process Manager: Process Failed to Complete Initialization alarm, refer to the [“Process Manager: Process Failed to Complete Initialization - Maintenance \(23\)” section on page 7-82](#).

## Process Manager: Restarting Process - Maintenance (24)

The Process Manager: Restarting Process alarm (minor) indicates the a PMG process is being restarted. To troubleshoot and correct the cause of the Process Manager: Restarting Process alarm, refer to the [“Process Manager: Restarting Process - Maintenance \(24\)” section on page 7-82](#).

## Process Manager: Changing State - Maintenance (25)

The Process Manager: Changing State event functions as an informational alert that a PMG process is changing state. The primary cause of the event is that a side is transitioning from one state to another. This is part of the normal side state change process. Monitor the system for other maintenance category event reports to see if the transition is due to a failure of a component within the specified side.

## Process Manager: Going Faulty - Maintenance (26)

The Process Manager: Going Faulty alarm (major) indicates that a PMG process is going faulty. To troubleshoot and correct the cause of the Process Manager: Going Faulty alarm, refer to the [“Process Manager: Going Faulty - Maintenance \(26\)” section on page 7-82](#).

## Process Manager: Changing Over to Active - Maintenance (27)

The Process Manager: Changing Over to Active event functions as an informational alert that a PMG process is being changed to active. The primary cause of the event is that the specified platform instance was in the standby state and was changed to the active state either by program control or via user request. No action is necessary. This is part of the normal process of activating the platform.

## Process Manager: Changing Over to Standby - Maintenance (28)

The Process Manager: Changing Over to Standby event functions as an information alert that a PMG process is being changed to standby. The primary cause of the event is that the specified side was in the active state and was changed to the standby state, or is being restored to service, and its mate is already in the active state either by program control or via user request. No action is necessary. This is part of the normal process of restoring or duplexing the platform.

## Administrative State Change Failure - Maintenance (29)

The Administrative State Change Failure event functions as a warning that a change of the administrative state has failed. The primary cause of the event is that an attempt to change the administrative state of a device has failed. If one is found, analyze the cause of the failure. Verify that the controlling element of the targeted device was in the ACTIVE state in order to service the request to change the ADMIN state of the device. If the controlling platform instance is not ACTIVE, restore it to service.

## Element Manager State Change - Maintenance (30)

The Element Manager State Change event functions as an informational alert that the element manager has changed state. The primary cause of the event is that the specified EMS has changed to the indicated state either naturally or via user request. The event is informational and no action is necessary. This is part of the normal state transitioning process for the EMS. Monitor the system for related event reports if the transition was due to a faulty or out of service state.

## Process Manager: Sending Go Active to Process - Maintenance (32)

The Process Manager: Sending Go Active to Process event functions as an informational alert that a process is being notified to switch to active state as the system is switching over from standby to active. The event is informational and no further action is required.

## Process Manager: Sending Go Standby to Process - Maintenance (33)

The Process Manager: Sending Go Standby to Process event functions as an informational alert that a process is being notified to exit gracefully as the system is switching over to standby state, or is shutting down. The switchover or shutdown could be due to the operator taking the action to switch or shut down the system or due to the system has detected a fault. The event is informational and no further action is required.

## Process Manager: Sending End Process to Process - Maintenance (34)

The Process Manager: Sending End Process to Process event functions as an informational alert that a process is being notified to exit gracefully as the system is switching over to standby state, or is shutting down. The switchover or shutdown could be due to the operator taking the action to switch or shut down the system or due to the system has detected a fault. The event is informational and no further action is required.

## Process Manager: All Processes Completed Initialization - Maintenance (35)

The Process Manager: All Processes Completed Initialization event functions as an informational alert that the system is being brought up, and that all processes are ready to start executing. The event is informational and no further action is required.

## Process Manager: Sending All Processes Initialization Complete to Process - Maintenance (36)

The Process Manager: Sending All Processes Initialization Complete to Process event functions as an informational alert that system is being brought up, and all processes are being notified to start executing. The event is informational and no further action is required.

## Process Manager: Killing Process - Maintenance (37)

The Process Manager: Killing Process event functions as an informational alert that a process is being killed. A software problem occurred while the system was being brought up or shut down. Either a process did not come up when the system was brought up and had to be killed in order to restart it or a process did not come up when the system was brought up and had to be killed in order to restart it. The event is informational and no further action is required.

## Process Manager: Clearing the Database - Maintenance (38)

The Process Manager: Clearing the Database event functions as an informational alert that the system is preparing to copy data from the mate. The system has been brought up and the mate side is running. The event is informational and no further action is required.

## Process Manager: Cleared the Database - Maintenance (39)

The Process Manager: Cleared the Database event functions as an informational alert that the system is prepared to copy data from the mate. The system has been brought up and the mate side is running. The event is informational and no further action is required.

## Process Manager: Binary Does not Exist for Process - Maintenance (40)

The Process Manager: Binary Does not Exist for Process alarm (critical) indicates that the platform was not installed correctly. To troubleshoot and correct the cause of the Process Manager: Binary Does not Exist for Process alarm, refer to the [“Process Manager: Binary Does not Exist for Process - Maintenance \(40\)” section on page 7-82.](#)

## Administrative State Change Successful with Warning - Maintenance (41)

The Administrative State Change Successful with Warning event functions as a warning that the system was in a flux when a successful administrative state change occurred. The primary cause of the event is that the system was in flux state when an administrative change state command was issued. To correct the primary cause of the event, retry the command.

## Number of Heartbeat Messages Received is Less Than 50% of Expected - Maintenance (42)

The Number of Heartbeat messages Received is Less Than 50% of Expected alarm (major) indicates that number of heartbeat (HB) messages being received is less than 50% of expected number. To troubleshoot and correct the cause of the Number of Heartbeat messages Received is Less Than 50% of Expected alarm, refer to the [“Number of Heartbeat Messages Received is Less Than 50% of Expected - Maintenance \(42\)” section on page 7-83.](#)

## Process Manager: Process Failed to Come Up in Active Mode - Maintenance (43)

The Process Manager: Process Failed to Come Up in Active Mode alarm (critical) indicates that the process has failed to come up in active mode. To troubleshoot and correct the cause of the Process Manager: Process Failed to Come Up in Active Mode alarm, refer to the [“Process Manager: Process Failed to Come Up in Active Mode - Maintenance \(43\)” section on page 7-83.](#)

## Process Manager: Process Failed to Come Up in Standby Mode - Maintenance (44)

The Process Manager: Process Failed to Come Up in Standby Mode alarm (critical) indicates that the process has failed to come up in standby mode. To troubleshoot and correct the cause of the Process Manager: Process Failed to Come Up in Standby Mode alarm, refer to the [“Process Manager: Process Failed to Come Up in Standby Mode - Maintenance \(44\)” section on page 7-83.](#)

## Application Instance State Change Failure - Maintenance (45)

The Application Instance State Change Failure alarm (major) indicates that an application instance state change failed. To troubleshoot and correct the cause of the Application Instance State Change Failure alarm, refer to the [“Application Instance State Change Failure - Maintenance \(45\)” section on page 7-83.](#)



## Network Interface Restored - Maintenance (46)

The Network Interface Restored event functions as an informational alert that the network interface was restored. The primary cause of the event is that the interface cable is reconnected and the interface is put 'up' using `ifconfig` command. The event is informational and no further action is required.

## Thread Watchdog Counter Expired for a Thread - Maintenance (47)

The Thread Watchdog Counter Expired for a Thread alarm (critical) indicates that a thread watchdog counter has expired for a thread. To troubleshoot and correct the cause of the Thread Watchdog Counter Expired for a Thread alarm, refer to the [“Thread Watchdog Counter Expired for a Thread - Maintenance \(47\)” section on page 7-83](#).

## Index Table Usage Exceeded Minor Usage Threshold Level - Maintenance (48)

The Index Table Usage Exceeded Minor Usage Threshold Level alarm (minor) indicates that the index (IDX) table usage has exceeded the minor threshold crossing usage level. To troubleshoot and correct the cause of the Index Table Usage Exceeded Minor Usage Threshold Level alarm, refer to the [“Index Table Usage Exceeded Minor Usage Threshold Level - Maintenance \(48\)” section on page 7-84](#).

## Index Table Usage Exceeded Major Usage Threshold Level - Maintenance (49)

The Index Table Usage Exceeded Major Usage Threshold Level alarm (major) indicates that the IDX table usage has exceeded the major threshold crossing usage level. To troubleshoot and correct the cause of the Index Table Usage Exceeded Major Usage Threshold Level alarm, refer to the [“Index Table Usage Exceeded Major Usage Threshold Level - Maintenance \(49\)” section on page 7-84](#).

## Index Table Usage Exceeded Critical Usage Threshold Level - Maintenance (50)

The Index Table Usage Exceeded Critical Usage Threshold Level alarm (critical) indicates that the IDX table usage has exceeded the critical threshold crossing usage level. To troubleshoot and correct the cause of the Index Table Usage Exceeded Critical Usage Threshold Level alarm, refer to the [“Index Table Usage Exceeded Critical Usage Threshold Level - Maintenance \(50\)” section on page 7-84](#).

## A Process Exceeds 70% of Central Processing Unit Usage - Maintenance (51)

The A Process Exceeds 70% of Central Processing Unit Usage alarm (major) indicates that a process has exceeded the CPU usage threshold of 70 percent. To troubleshoot and correct the cause of the A Process Exceeds 70% of Central Processing Unit Usage alarm, refer to the [“A Process Exceeds 70% of Central Processing Unit Usage - Maintenance \(51\)” section on page 7-84](#).

## Central Processing Unit Usage is Now Below the 50% Level - Maintenance (52)

The Central Processing Unit Usage is Now Below the 50% Level event functions as an informational alert that the CPU usage level has fallen below the threshold level of 50 percent. The event is informational and no further action is required.

## The Central Processing Unit Usage is Over 90% Busy - Maintenance (53)

The Central Processing Unit Usage is Over 90% Busy alarm (critical) indicates that the CPU usage is over the threshold level of 90 percent. To troubleshoot and correct the cause of The Central Processing Unit Usage is Over 90% Busy alarm, refer to the [“The Central Processing Unit Usage is Over 90% Busy - Maintenance \(53\)” section on page 7-84.](#)

## The Central Processing Unit has Returned to Normal Levels of Operation - Maintenance (54)

The The Central Processing Unit has Returned to Normal Levels of Operation event functions as an informational alert that the CPU usage has returned to the normal level of operation. The event is informational and no further actions is required.

## The Five Minute Load Average is Abnormally High - Maintenance (55)

The Five Minute Load Average is Abnormally High alarm (major) indicates the five minute load average is abnormally high. To troubleshoot and correct the cause of The Five Minute Load Average is Abnormally High alarm, refer to the [“The Five Minute Load Average is Abnormally High - Maintenance \(55\)” section on page 7-85.](#)

## The Load Average has Returned to Normal Levels - Maintenance (56)

The Load Average has Returned to Normal Levels event functions as an informational alert the load average has returned to normal levels. The event is informational and no further action is required.

## Memory and Swap are Consumed at Critical Levels - Maintenance (57)



### Note

---

Maintenance (57) is issued by the BTS 10200 system when memory consumption is greater than 95 percent (>95%) and swap space consumption is greater than 50 percent (>50%).

---

The Memory and Swap are Consumed at Critical Levels alarm (critical) indicates that memory and swap file usage have reached critical levels. To troubleshoot and correct the cause of the Memory and Swap are Consumed at Critical Levels alarm, refer to the [“Memory and Swap are Consumed at Critical Levels - Maintenance \(57\)” section on page 7-85.](#)

## Memory and Swap are Consumed at Abnormal Levels - Maintenance (58)

**Note**

Maintenance (58) is issued by the BTS 10200 system when memory consumption is greater than 80 percent (>80%) and swap space consumption is greater than 30 percent (>30%).

The Memory and Swap are Consumed at Abnormal Levels event functions as an informational alert the memory and swap file usage are being consumed at abnormal levels. The primary cause of the event is that a process or multiple processes have consumed an abnormal amount of memory on the system and the operating system is utilizing an abnormal amount of the swap space for process execution. This can be a result of high call rates or bulk provisioning activity. Monitor the system to ensure all subsystems are performing normally. If so, only lightening the effective load on the system will clear the situation. If not, verify which process(es) are running at abnormally high rates, and contact Cisco TAC. Refer to the [“Obtaining Technical Assistance”](#) section on page xxxviii for detailed instructions on contacting Cisco TAC and opening a service request.

## No Heartbeat Messages Received Through the Interface - Maintenance (61)

The No Heartbeat Messages Received Through the Interface alarm (critical) indicates that no HB messages are being received through the local network interface. To troubleshoot and correct the cause of the No Heartbeat Messages Received Through the Interface alarm, refer to the [“No Heartbeat Messages Received Through the Interface - Maintenance \(61\)”](#) section on page 7-85.

## Link Monitor: Interface Lost Communication - Maintenance (62)

The Link Monitor: Interface Lost Communication alarm (major) indicates that a interface has lost communication. To troubleshoot and correct the cause of the Link Monitor: Interface Lost Communication alarm, refer to the [“Link Monitor: Interface Lost Communication - Maintenance \(62\)”](#) section on page 7-85.

## Outgoing Heartbeat Period Exceeded Limit - Maintenance (63)

The Outgoing Heartbeat Period Exceeded Limit alarm (major) indicates that the outgoing HB period has exceeded the limit. To troubleshoot and correct the cause of the Outgoing Heartbeat Period Exceeded Limit alarm, refer to the [“Outgoing Heartbeat Period Exceeded Limit - Maintenance \(63\)”](#) section on page 7-86.

## Average Outgoing Heartbeat Period Exceeds Major Alarm Limit - Maintenance (64)

The Average Outgoing Heartbeat Period Exceeds Major Alarm Limit alarm (major) indicates that the average outgoing HB period has exceeded the major threshold crossing alarm limit. To troubleshoot and correct the cause of the Average Outgoing Heartbeat Period Exceeds Major Alarm Limit alarm, refer to the [“Average Outgoing Heartbeat Period Exceeds Major Alarm Limit - Maintenance \(64\)”](#) section on page 7-86.

## Disk Partition Critically Consumed - Maintenance (65)

The Disk Partition Critically Consumed alarm (critical) indicates that the disk partition consumption has reached critical limits. To troubleshoot and correct the cause of the Disk Partition Critically Consumed alarm, refer to the [“Disk Partition Critically Consumed - Maintenance \(65\)”](#) section on page 7-86.

## Disk Partition Significantly Consumed - Maintenance (66)

The Disk Partition Significantly Consumed alarm (major) indicates that the disk partition consumption has reached the major threshold crossing level. To troubleshoot and correct the cause of the Disk Partition Significantly Consumed alarm, refer to the [“Disk Partition Significantly Consumed - Maintenance \(66\)”](#) section on page 7-86.

## The Free Inter-Process Communication Pool Buffers Below Minor Threshold - Maintenance (67)

The Free Inter-Process Communication Pool Buffers Below Minor Threshold alarm (minor) indicates that the number of free IPC pool buffers has fallen below the minor threshold crossing level. To troubleshoot and correct the cause of The Free Inter-Process Communication Pool Buffers Below Minor Threshold alarm, refer to the [“The Free Inter-Process Communication Pool Buffers Below Minor Threshold - Maintenance \(67\)”](#) section on page 7-86.

## The Free Inter-Process Communication Pool Buffers Below Major Threshold - Maintenance (68)

The Free Inter-Process Communication Pool Buffers Below Major Threshold alarm (major) indicates that the number of free IPC pool buffers has fallen below the major threshold crossing level. To troubleshoot and correct the cause of The Free Inter-Process Communication Pool Buffers Below Major Threshold alarm, refer to the [“The Free Inter-Process Communication Pool Buffers Below Major Threshold - Maintenance \(68\)”](#) section on page 7-87.

## The Free Inter-Process Communication Pool Buffers Below Critical Threshold - Maintenance (69)

The Free Inter-Process Communication Pool Buffers Below Critical Threshold alarm (critical) indicates that the number of free IPC pool buffers has fallen below the critical threshold crossing level. To troubleshoot and correct the cause of The Free Inter-Process Communication Pool Buffers Below Critical Threshold alarm, refer to the [“The Free Inter-Process Communication Pool Buffers Below Critical Threshold - Maintenance \(69\)”](#) section on page 7-87.

## The Free Inter-Process Communication Pool Buffer Count Below Minimum Required - Maintenance (70)

The Free Inter-Process Communication Pool Buffers Below Critical Threshold alarm (critical) indicates that the IPC pool buffers are not being freed properly by the application or the application is not able to keep up with the incoming IPC messaging traffic. To troubleshoot and correct the cause of The Free Inter-Process Communication Pool Buffers Below Critical Threshold alarm, refer to the [“The Free Inter-Process Communication Pool Buffer Count Below Minimum Required - Maintenance \(70\)”](#) section on page 7-87.

## Local Domain Name System Server Response Too Slow - Maintenance (71)

The Local Domain Name System Server Response Too Slow alarm (major) indicates that the response time of the local DNS server is too slow. To troubleshoot and correct the cause of the Local Domain Name System Server Response Too Slow alarm, refer to the [“Local Domain Name System Server Response Too Slow - Maintenance \(71\)”](#) section on page 7-87.

## External Domain Name System Server Response Too Slow - Maintenance (72)

The External Domain Name System Server Response Too Slow alarm (major) indicates that the response time of the external DNS server is too slow. To troubleshoot and correct the cause of the External Domain Name System Server Response Too Slow alarm, refer to the [“External Domain Name System Server Response Too Slow - Maintenance \(72\)”](#) section on page 7-87.

## External Domain Name System Server not Responsive - Maintenance (73)

The External Domain Name System Server not Responsive alarm (critical) indicates that the external DNS server is not responding to network queries. To troubleshoot and correct the cause of the External Domain Name System Server not Responsive alarm, refer to the [“External Domain Name System Server not Responsive - Maintenance \(73\)”](#) section on page 7-88.

## Local Domain Name System Service not Responsive - Maintenance (74)

The Local Domain Name System Service not Responsive alarm (critical) indicates that the local DNS server is not responding to network queries. To troubleshoot and correct the cause of the Local Domain Name System Service not Responsive alarm, refer to the [“Local Domain Name System Service not Responsive - Maintenance \(74\)”](#) section on page 7-88.

## Mismatch of Internet Protocol Address Local Server and Domain Name System - Maintenance (75)

The Mismatch of Internet Protocol Address Local Server and Domain Name System event functions as a warning that a mismatch of the local server IP address and the DNS server address has occurred. The primary cause of the event is that the DNS server updates are not getting to the Cisco BTS 10200 Softswitch from the external server, or the discrepancy was detected before the local DNS lookup table was updated. Ensure the external DNS server is operational and sending updates to the Cisco BTS 10200 Softswitch.

## Mate Time Differs Beyond Tolerance - Maintenance (77)

The Mate Time Differs Beyond Tolerance alarm (major) indicates that the mate differs beyond the tolerance. To troubleshoot and correct the cause of the Mate Time Differs Beyond Tolerance alarm, refer to the [“Mate Time Differs Beyond Tolerance - Maintenance \(77\)” section on page 7-88](#).

## Bulk Data Management System Admin State Change - Maintenance (78)

The Bulk Data Management System Admin State Change event functions as an informational alert that the BDMS administrative state has changed. The primary cause of the event is that the Bulk Data Management Server was switched over manually. The event is informational and no further action is required.

## Resource Reset - Maintenance (79)

The Resource Reset event functions as an informational alert that a resource reset has occurred. The event is informational and no further action is required.

## Resource Reset Warning - Maintenance (80)

The Resource Reset Warning event functions as an informational alert that a resource reset is about to occur. The event is informational and no further action is required.

## Resource Reset Failure - Maintenance (81)

The Resource Reset Failure event functions as an informational alert that a resource reset has failed. The primary cause of the event is an internal messaging error. Check dataword three (failure reason) to determine if this is caused by invalid user input, inconsistent provisioning of the device, or if the system is busy and a timeout occurred.

## Average Outgoing Heartbeat Period Exceeds Critical Limit - Maintenance (82)

The Average Outgoing Heartbeat Period Exceeds Critical Limit alarm (critical) indicates that the average outgoing HB period has exceeded the critical limit threshold. To troubleshoot and correct the cause of the Average Outgoing Heartbeat Period Exceeds Critical Limit alarm, refer to the [“Average Outgoing Heartbeat Period Exceeds Critical Limit - Maintenance \(82\)”](#) section on page 7-88.

## Swap Space Below Minor Threshold - Maintenance (83)

The Swap Space Below Minor Threshold alarm (minor) indicates that the swap space has fallen below the minor threshold level. To troubleshoot and correct the cause of the Swap Space Below Minor Threshold alarm, refer to the [“Swap Space Below Minor Threshold - Maintenance \(83\)”](#) section on page 7-88.

## Swap Space Below Major Threshold - Maintenance (84)

The Swap Space Below Major Threshold alarm (major) indicates that the swap space has fallen below the major threshold level. To troubleshoot and correct the cause of the Swap Space Below Major Threshold alarm, refer to the [“Swap Space Below Major Threshold - Maintenance \(84\)”](#) section on page 7-88.

## Swap Space Below Critical Threshold - Maintenance (85)

The Swap Space Below Critical Threshold alarm (critical) indicates that the swap space has fallen below the critical threshold level. To troubleshoot and correct the cause of the Swap Space Below Major Threshold alarm, refer to the [“Swap Space Below Critical Threshold - Maintenance \(85\)”](#) section on page 7-89.

## System Health Report Collection Error - Maintenance (86)

The System Health Report Collection Error alarm (minor) indicates that an error occurred while collecting System Health Report. To troubleshoot and correct the cause of the System Health Report Collection Error alarm, refer to the [“System Health Report Collection Error - Maintenance \(86\)”](#) section on page 7-89.

## Status Update Process Request Failed - Maintenance (87)

The Status Update Process Request Failed alarm (major) indicates that the status update process request failed. To troubleshoot and correct the cause of the Status Update Process Request Failed alarm, refer to the [“Status Update Process Request Failed - Maintenance \(87\)”](#) section on page 7-89.

## Status Update Process Database List Retrieval Error - Maintenance (88)

The Status Update Process Database List Retrieval Error alarm (major) indicates that the status update process DB had a retrieval error. To troubleshoot and correct the cause of the Status Update Process Database List Retrieval Error alarm, refer to the [“Status Update Process Database List Retrieval Error - Maintenance \(88\)”](#) section on page 7-89.

## Status Update Process Database Update Error - Maintenance (89)

The Status Update Process Database Update Error alarm (major) indicates that the status update process DB had an update error. To troubleshoot and correct the cause of the Status Update Process Database Update Error alarm, refer to the [“Status Update Process Database Update Error - Maintenance \(89\)”](#) section on page 7-89.

## Disk Partition Moderately Consumed - Maintenance (90)

The Disk Partition Moderately Consumed alarm (minor) indicates that the disk partition is moderately consumed. To troubleshoot and correct the cause of the Disk Partition Moderately Consumed alarm, refer to the [“Disk Partition Moderately Consumed - Maintenance \(90\)”](#) section on page 7-89.

## Internet Protocol Manager Configuration File Error - Maintenance (91)

The Internet Protocol Manager Configuration File Error alarm (critical) indicates that IPM configuration file has an error. To troubleshoot and correct the cause of the Internet Protocol Manager Configuration File Error alarm, refer to the [“Internet Protocol Manager Configuration File Error - Maintenance \(91\)”](#) section on page 7-90.

## Internet Protocol Manager Initialization Error - Maintenance (92)

The Internet Protocol Manager Initialization Error alarm (major) indicates that the IPM process failed to initialize correctly. To troubleshoot and correct the cause of the Internet Protocol Manager Initialization Error alarm, refer to the [“Internet Protocol Manager Initialization Error - Maintenance \(92\)”](#) section on page 7-90.

## Internet Protocol Manager Interface Failure - Maintenance (93)

The Internet Protocol Manager Interface Failure alarm (major) indicates that an IPM interface has failed. To troubleshoot and correct the cause of the Internet Protocol Manager Interface Failure alarm, refer to [“Internet Protocol Manager Interface Failure - Maintenance \(93\)”](#) section on page 7-90.

## Internet Protocol Manager Interface State Change - Maintenance (94)

The Internet Protocol Manager Interface State Change event functions as an informational alert that the state of the IPM interface has changed. The primary cause of the event is that the IPM changed state on an interface (up or down). The event is informational and no further action is required.



## Internet Protocol Manager Interface Created - Maintenance (95)

The Internet Protocol Manager Interface Created event functions as an informational alert that the IPM has created a new logical interface. The event is informational and no further action is required.

## Internet Protocol Manager Interface Removed - Maintenance (96)

The Internet Protocol Manager Interface Removed event functions as an informational alert that the IPM has removed a logical interface. The event is informational and no further action is required.

## Inter-Process Communication Input Queue Entered Throttle State - Maintenance (97)

The Inter-Process Communication Input Queue Entered Throttle State alarm (critical) alarm indicates that the thread is not able to process its IPC input messages fast enough, hence the input queue has grown too large and is using up too much of the IPC memory pool resource. To troubleshoot and correct the cause of the Inter-Process Communication Input Queue Entered Throttle State alarm, refer to the [“Inter-Process Communication Input Queue Entered Throttle State - Maintenance \(97\)”](#) section on page 7-90.

## Inter-Process Communication Input Queue Depth at 25% of its Hi-Watermark - Maintenance (98)

The Inter-Process Communication Input Queue Depth at 25% of its Hi-Watermark alarm (minor) indicates that the IPC input queue depth has reached 25 percent of its hi-watermark. To troubleshoot and correct the cause of the Inter-Process Communication Input Queue Depth at 25% of its Hi-Watermark alarm, refer to the [“Inter-Process Communication Input Queue Depth at 25% of Its Hi-Watermark - Maintenance \(98\)”](#) section on page 7-90.

## Inter-Process Communication Input Queue Depth at 50% of its Hi-Watermark - Maintenance (99)

The Inter-Process Communication Input Queue Depth at 50% of its Hi-Watermark alarm (major) indicates that the IPC input queue depth has reached 50 percent of its hi-watermark. To troubleshoot and correct the cause of the Inter-Process Communication Input Queue Depth at 50% of its Hi-Watermark alarm, refer to the [“Inter-Process Communication Input Queue Depth at 50% of Its Hi-Watermark - Maintenance \(99\)”](#) section on page 7-91.

## Inter-Process Communication Input Queue Depth at 75% of its Hi-Watermark - Maintenance (100)

The Inter-Process Communication Input Queue Depth at 75% of its Hi-Watermark alarm (critical) indicates that the IPC input queue depth has reached 75 percent of its hi-watermark. To troubleshoot and correct the cause of the Inter-Process Communication Input Queue Depth at 75% of its Hi-Watermark alarm, refer to the [“Inter-Process Communication Input Queue Depth at 75% of Its Hi-Watermark - Maintenance \(100\)”](#) section on page 7-91.

## Switchover in Progress - Maintenance (101)

The Switchover in Progress alarm (critical) indicates that a system switchover is progress. This alarm is issued when a system switchover is in progress either due to manual switchover (via CLI command), failover switchover, or automatic switchover. No action needs to be taken, the alarm is cleared when switchover is complete. Service is temporarily suspended for a short period of time during this transition.

## Thread Watchdog Counter Close to Expiry for a Thread - Maintenance (102)

The Thread Watchdog Counter Close to Expiry for a Thread alarm (critical) indicates that the thread watchdog counter is close to expiry for a thread. The primary cause of the alarm is that a software error has occurred. No further action is required, the Cisco BTS 10200 Softswitch system will automatically recover or shutdown.

## Central Processing Unit is Offline - Maintenance (103)

The Central Processing Unit is Offline alarm (critical) indicates that the CPU is offline. To troubleshoot and correct the cause of the Central Processing Unit is Offline alarm, refer to the [“Central Processing Unit is Offline - Maintenance \(103\)”](#) section on page 7-91.

# Troubleshooting Maintenance Alarms

This section provides the information needed to troubleshoot and correct Maintenance alarms. [Table 7-3](#) lists all Maintenance alarms in numerical order and provides cross reference to each subsection in this section.

**Table 7-3** Cisco BTS 10200 Softswitch Maintenance Alarms

| Alarm Type      | Alarm Name                                                                                            | Alarm Severity |
|-----------------|-------------------------------------------------------------------------------------------------------|----------------|
| MAINTENANCE(3)  | <a href="#">Local Side has Become Faulty - Maintenance (3)</a>                                        | MAJOR          |
| MAINTENANCE(4)  | <a href="#">Mate Side has Become Faulty - Maintenance (4)</a>                                         | MAJOR          |
| MAINTENANCE(5)  | <a href="#">Changeover Failure - Maintenance (5)</a>                                                  | MAJOR          |
| MAINTENANCE(6)  | <a href="#">Changeover Timeout - Maintenance (6)</a>                                                  | MAJOR          |
| MAINTENANCE(7)  | <a href="#">Mate Rejected Changeover - Maintenance (7)</a>                                            | MAJOR          |
| MAINTENANCE(8)  | <a href="#">Mate Changeover Timeout - Maintenance (8)</a>                                             | MAJOR          |
| MAINTENANCE(9)  | <a href="#">Local Initialization Failure - Maintenance (9)</a>                                        | MAJOR          |
| MAINTENANCE(10) | <a href="#">Local Initialization Timeout - Maintenance (10)</a>                                       | MAJOR          |
| MAINTENANCE(18) | <a href="#">Process Manager: Process has Died - Maintenance (18)</a>                                  | MINOR          |
| MAINTENANCE(19) | <a href="#">Process Manager: Process Exceeded Restart Rate - Maintenance (19)</a>                     | MAJOR          |
| MAINTENANCE(20) | <a href="#">Lost Connection to Mate - Maintenance (20)</a>                                            | MAJOR          |
| MAINTENANCE(21) | <a href="#">Network Interface Down - Maintenance (21)</a>                                             | MAJOR          |
| MAINTENANCE(23) | <a href="#">Process Manager: Process Failed to Complete Initialization - Maintenance (23)</a>         | MAJOR          |
| MAINTENANCE(24) | <a href="#">Process Manager: Restarting Process - Maintenance (24)</a>                                | MINOR          |
| MAINTENANCE(26) | <a href="#">Process Manager: Going Faulty - Maintenance (26)</a>                                      | MAJOR          |
| MAINTENANCE(40) | <a href="#">Process Manager: Binary Does not Exist for Process - Maintenance (40)</a>                 | CRITICAL       |
| MAINTENANCE(42) | <a href="#">Number of Heartbeat Messages Received is Less Than 50% of Expected - Maintenance (42)</a> | MAJOR          |
| MAINTENANCE(43) | <a href="#">Process Manager: Process Failed to Come Up in Active Mode - Maintenance (43)</a>          | CRITICAL       |
| MAINTENANCE(44) | <a href="#">Process Manager: Process Failed to Come Up in Standby Mode - Maintenance (44)</a>         | CRITICAL       |
| MAINTENANCE(45) | <a href="#">Application Instance State Change Failure - Maintenance (45)</a>                          | MAJOR          |
| MAINTENANCE(47) | <a href="#">Thread Watchdog Counter Expired for a Thread - Maintenance (47)</a>                       | CRITICAL       |
| MAINTENANCE(48) | <a href="#">Index Table Usage Exceeded Minor Usage Threshold Level - Maintenance (48)</a>             | MINOR          |
| MAINTENANCE(49) | <a href="#">Index Table Usage Exceeded Major Usage Threshold Level - Maintenance (49)</a>             | MAJOR          |
| MAINTENANCE(50) | <a href="#">Index Table Usage Exceeded Critical Usage Threshold Level - Maintenance (50)</a>          | CRITICAL       |
| MAINTENANCE(51) | <a href="#">A Process Exceeds 70% of Central Processing Unit Usage - Maintenance (51)</a>             | MAJOR          |
| MAINTENANCE(53) | <a href="#">The Central Processing Unit Usage is Over 90% Busy - Maintenance (53)</a>                 | CRITICAL       |
| MAINTENANCE(55) | <a href="#">The Five Minute Load Average is Abnormally High - Maintenance (55)</a>                    | MAJOR          |
| MAINTENANCE(57) | <a href="#">Memory and Swap are Consumed at Critical Levels - Maintenance (57)</a>                    | CRITICAL       |
| MAINTENANCE(61) | <a href="#">No Heartbeat Messages Received Through the Interface - Maintenance (61)</a>               | CRITICAL       |
| MAINTENANCE(62) | <a href="#">Link Monitor: Interface Lost Communication - Maintenance (62)</a>                         | MAJOR          |

**Table 7-3 Cisco BTS 10200 Softswitch Maintenance Alarms (continued)**

| Alarm Type       | Alarm Name                                                                                       | Alarm Severity |
|------------------|--------------------------------------------------------------------------------------------------|----------------|
| MAINTENANCE(63)  | Outgoing Heartbeat Period Exceeded Limit - Maintenance (63)                                      | MAJOR          |
| MAINTENANCE(64)  | Average Outgoing Heartbeat Period Exceeds Major Alarm Limit - Maintenance (64)                   | MAJOR          |
| MAINTENANCE(65)  | Disk Partition Critically Consumed - Maintenance (65)                                            | CRITICAL       |
| MAINTENANCE(66)  | Disk Partition Significantly Consumed - Maintenance (66)                                         | MAJOR          |
| MAINTENANCE(67)  | The Free Inter-Process Communication Pool Buffers Below Minor Threshold - Maintenance (67)       | MINOR          |
| MAINTENANCE(68)  | The Free Inter-Process Communication Pool Buffers Below Major Threshold - Maintenance (68)       | MAJOR          |
| MAINTENANCE(69)  | The Free Inter-Process Communication Pool Buffers Below Critical Threshold - Maintenance (69)    | CRITICAL       |
| MAINTENANCE(70)  | The Free Inter-Process Communication Pool Buffer Count Below Minimum Required - Maintenance (70) | CRITICAL       |
| MAINTENANCE(71)  | Local Domain Name System Server Response Too Slow - Maintenance (71)                             | MAJOR          |
| MAINTENANCE(72)  | External Domain Name System Server Response Too Slow - Maintenance (72)                          | MAJOR          |
| MAINTENANCE(73)  | External Domain Name System Server not Responsive - Maintenance (73)                             | CRITICAL       |
| MAINTENANCE(74)  | Local Domain Name System Service not Responsive - Maintenance (74)                               | CRITICAL       |
| MAINTENANCE(77)  | Mate Time Differs Beyond Tolerance - Maintenance (77)                                            | MAJOR          |
| MAINTENANCE(82)  | Average Outgoing Heartbeat Period Exceeds Critical Limit - Maintenance (82)                      | CRITICAL       |
| MAINTENANCE(83)  | Swap Space Below Minor Threshold - Maintenance (83)                                              | MINOR          |
| MAINTENANCE(84)  | Swap Space Below Major Threshold - Maintenance (84)                                              | MAJOR          |
| MAINTENANCE(85)  | Swap Space Below Critical Threshold - Maintenance (85)                                           | CRITICAL       |
| MAINTENANCE(86)  | System Health Report Collection Error - Maintenance (86)                                         | MINOR          |
| MAINTENANCE(87)  | Status Update Process Request Failed - Maintenance (87)                                          | MAJOR          |
| MAINTENANCE(88)  | Status Update Process Database List Retrieval Error - Maintenance (88)                           | MAJOR          |
| MAINTENANCE(89)  | Status Update Process Database Update Error - Maintenance (89)                                   | MAJOR          |
| MAINTENANCE(90)  | Disk Partition Moderately Consumed - Maintenance (90)                                            | MINOR          |
| MAINTENANCE(91)  | Internet Protocol Manager Configuration File Error - Maintenance (91)                            | CRITICAL       |
| MAINTENANCE(92)  | Internet Protocol Manager Initialization Error - Maintenance (92)                                | MAJOR          |
| MAINTENANCE(93)  | Internet Protocol Manager Interface Failure - Maintenance (93)                                   | MAJOR          |
| MAINTENANCE(97)  | Inter-Process Communication Input Queue Entered Throttle State - Maintenance (97)                | CRITICAL       |
| MAINTENANCE(98)  | Inter-Process Communication Input Queue Depth at 25% of Its Hi-Watermark - Maintenance (98)      | MINOR          |
| MAINTENANCE(99)  | Inter-Process Communication Input Queue Depth at 50% of Its Hi-Watermark - Maintenance (99)      | MAJOR          |
| MAINTENANCE(100) | Inter-Process Communication Input Queue Depth at 75% of Its Hi-Watermark - Maintenance (100)     | CRITICAL       |
| MAINTENANCE(101) | Switchover in Progress - Maintenance (101)                                                       | CRITICAL       |

**Table 7-3 Cisco BTS 10200 Softswitch Maintenance Alarms (continued)**

| Alarm Type       | Alarm Name                                                                               | Alarm Severity |
|------------------|------------------------------------------------------------------------------------------|----------------|
| MAINTENANCE(102) | <a href="#">Thread Watchdog Counter Close to Expiry for a Thread - Maintenance (102)</a> | CRITICAL       |
| MAINTENANCE(103) | <a href="#">Central Processing Unit is Offline - Maintenance (103)</a>                   | CRITICAL       |

## Local Side has Become Faulty - Maintenance (3)

The Local Side has Become Faulty alarm (major) indicates that the local side has become faulty. The alarm can result from maintenance reports 5, 6, 9, 10, 19, or 20. Review information from CLI log report. The alarm is usually caused by a software problem. To correct the primary cause of the alarm, restart the software using the Installation and Startup procedure. The alarm can also be caused by manually shutting down the system using platform stop command. To correct the secondary cause of the alarm, reboot host machine, reinstall all applications and restart all applications. If the alarm is reoccurring, the operating system or the hardware may have a problem.

## Mate Side has Become Faulty - Maintenance (4)

The Mate Side has Become Faulty alarm (major) indicates that the mate side has become faulty. The primary cause of the alarm is that the local side has detected the mate side going into a faulty state. To correct the primary cause of the alarm, display the event summary on the faulty mate side, using the **report event-summary** command (see the CLI Guide for command details). Review information in the event summary. The alarm is usually caused by a software problem. After confirming the active side is processing traffic, restart software on the mate side. Log in to the mate platform as root user. Enter platform stop command and then platform start command. If a software restart does not resolve the problem or if the platform goes immediately to faulty again, or does not start, contact Cisco TAC. It may be necessary to reinstall software. If the alarm is reoccurring, then the operating system or the hardware may have a problem. Reboot host machine, then reinstall and restart all applications. The reboot will bring down the other applications running on the machine. Contact Cisco TAC for assistance. Refer to the [“Obtaining Technical Assistance” section on page xxxviii](#) for detailed instructions on contacting Cisco TAC and opening a service request.

## Changeover Failure - Maintenance (5)

The Changeover Failure alarm (major) indicates that a changeover failed. The alarm is issued when changing from an active processor to a standby processor and the changeover fails. To correct the cause of the alarm, review alarm information from CLI log report. This alarm is usually caused by a software problem on the specific platform identified in the alarm report. Restart the platform identified in the alarm report. If the platform restart is not successful, reinstall the application on the platform, and then restart platform again. If necessary, reboot host machine the platform is located on. Then reinstall and restart all applications on this machine. If faulty state is a reoccurring event, then operating system or the hardware may be defective. Contact Cisco TAC for assistance. It may also be helpful to gather information event/alarm reports that were issued before and after this alarm report. Refer to the [“Obtaining Technical Assistance” section on page xxxviii](#) for detailed instructions on contacting Cisco TAC and opening a service request.

## Changeover Timeout - Maintenance (6)

The Changeover Timeout alarm (major) indicates that a changeover timed out. The cause of the alarm is that the system failed to changeover within time period. Soon after this event is issued, one platform will go to faulty state. This alarm is usually caused by a software problem on the specific platform identified in the alarm report. To correct the cause of the alarm, review information from CLI log report. On the platform identified in this alarm report, restart the platform. If platform restart is not successful, reinstall the application for this platform, and then restart platform again. If necessary, reboot host machine the platform is located on. Then reinstall and restart all applications on this machine. If faulty state is a reoccurring event, then operating system or hardware may be defective. Contact Cisco TAC for assistance. It may also be helpful to gather information event/alarm reports that were issued before and after this alarm report. Refer to the [“Obtaining Technical Assistance” section on page xxxviii](#) for detailed instructions on contacting Cisco TAC and opening a service request.

## Mate Rejected Changeover - Maintenance (7)

The Mate Rejected Changeover alarm (major) indicates that the mate rejected the changeover. The primary cause of the alarm is that the mate is not in a stable state. To correct the primary cause of the alarm, enter the status command to get information on the two systems in the pair (primary and secondary EMS, CA or FS). The secondary cause of the alarm is that the mate detects that it is faulty during changeover and then rejects changeover.

To correct the secondary cause of the alarm, check to see if the mate is faulty (not running), then perform the corrective action steps listed in the [“Mate Side has Become Faulty - Maintenance \(4\)” section on page 7-77](#). Additionally, if both systems (local and mate) are still running, diagnose whether both instances are operating in stable state (one in active and the other in standby). If both are in a stable state, wait 10 minutes and try the “control” command again. If standby side is not in stable state, bring down the standby side and restart software using the “platform stop” and “platform start” commands. If software restart does not resolve the problem, or if the problem is commonly occurring, contact Cisco TAC. It may be necessary to reinstall software. Additional operating system or hardware problems may also need to be resolved. Refer to the [“Obtaining Technical Assistance” section on page xxxviii](#) for detailed instructions on contacting Cisco TAC and opening a service request.

To continue troubleshooting the cause of the alarm, refer to [Figure 7-1](#) if the forced switchover has been rejected by the secondary. Refer to [Figure 7-2](#) if the primary failed to come up in the active state.

**Figure 7-1**      **Corrective Action for Maintenance Event (7) (Mate Rejected Changeover)  
Forced Switchover Rejected By Secondary**

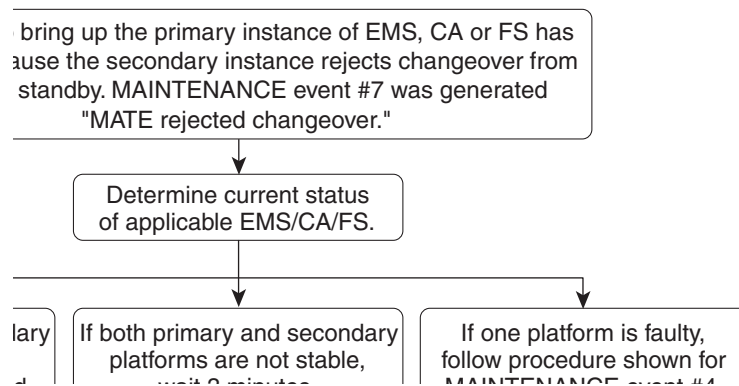
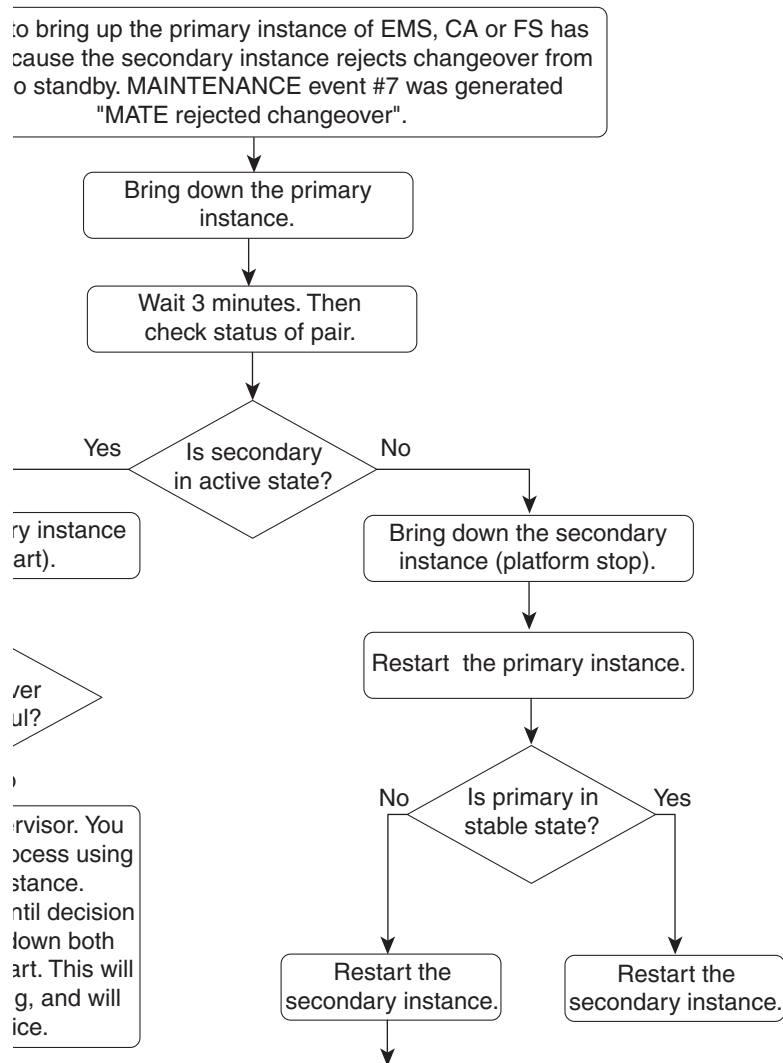


**Figure 7-2** *Corrective Action for Maintenance Event (7) (Mate Rejected Changeover)  
Primary Failed To Come Up in Active State*



**Note**

The attempted changeover could be caused by a forced (operator) switch, or it could be caused by secondary instance rejecting changeover as primary is being brought up.



## Mate Changeover Timeout - Maintenance (8)

The Mate Changeover Timeout alarm (major) indicates that the mate changeover timed out. The primary cause of the alarm is that the mate is faulty. This alarm is usually caused by a software problem on the specific mate platform identified in the alarm report. To correct the primary cause of the alarm, review information from CLI log report concerning faulty mate. On the mate platform identified in this alarm report, restart the platform. If mate platform restart is not successful, reinstall the application for this mate platform, and then restart mate platform again. If necessary, reboot host machine this mate platform is located on. Then reinstall and restart all applications on that machine.

## Local Initialization Failure - Maintenance (9)

The Local Initialization Failure alarm (major) indicates that the local initialization has failed. The primary cause of the alarm is that the local initialization has failed. When this alarm event report is issued, the system has failed and the re-initialization process has failed. To correct the primary cause of the alarm, check that the binary files are present for the unit (Call Agent, Feature Server, Element Manager). If the files are not present, then re-install the files from the initial or the backup media. Then restart the failed device.

## Local Initialization Timeout - Maintenance (10)

The Local Initialization Timeout alarm (major) indicates that the local initialization has timed out. The primary cause of this alarm is that the local initialization has timed out. When the event report is issued, the system has failed and the re-initialization process has failed. To correct the primary cause of the alarm, check that the binary files are present for the unit (Call Agent, Feature, Server, or Element Manager). If the files are not present, then re-install the files from initial or backup media. Then restart the failed device.

## Process Manager: Process has Died - Maintenance (18)

The Process Manager: Process has Died alarm (minor) indicates that a process has died. The primary cause of the alarm is that a software problem has occurred. If problem persists or is reoccurring, contact Cisco TAC. Refer to the [“Obtaining Technical Assistance” section on page xxxviii](#) for detailed instructions on contacting Cisco TAC and opening a service request.

## Process Manager: Process Exceeded Restart Rate - Maintenance (19)

The Process Manager: Process Exceeded Restart Rate alarm (major) indicates that a process has exceeded the restart rate. This alarm is usually caused by a software problem on the specific platform identified in the alarm report. Soon after this event is issued, one platform will go to faulty state. To correct the primary cause of the alarm, review the information from CLI log report. On the platform identified in this alarm report, restart the platform. If platform restart is not successful, reinstall the application for this platform, and then restart platform again. If necessary, reboot host machine this platform is located on. Then reinstall and restart all applications on this machine.

If faulty state is a commonly occurring event, then OS or hardware may be a problem. Contact Cisco TAC for assistance. It may also be helpful to gather information event/alarm reports that were issued before and after this alarm report.

## Lost Connection to Mate - Maintenance (20)

The Lost Connection to Mate alarm (major) indicates that the keepalive module connection to the mate has been lost. The primary cause of the alarm is that a network interface hardware problem was occurred. Soon after this event is issued, one platform may go to faulty state. To correct the primary cause of this alarm, check whether the network interface is down. If so, restore network interface and restart the software. The secondary cause of the alarm is a router problem. If secondary cause of the alarm is a router problem, then repair router and reinstall.

## Network Interface Down - Maintenance (21)

The Network Interface Down alarm (major) indicates that the network interface has gone down. The primary cause of the alarm is a network interface hardware problem. Soon after this alarm event is issued, one platform may go to faulty state. Subsequently system goes faulty. To correct the primary cause of the alarm, check whether the network interface is down. If so, restore network interface and restart the software.

## Process Manager: Process Failed to Complete Initialization - Maintenance (23)

The Process Manager: Process Failed to Complete Initialization alarm (major) indicates that a PMG process failed to complete initialization. The primary cause of the this alarm is that the specified process failed to complete initialization during the restoral process. To correct the primary cause of the alarm, verify that the specified process's binary image is installed. If not, install it and restart the platform.

## Process Manager: Restarting Process - Maintenance (24)

The Process Manager: Restarting Process alarm (minor) indicates the a PMG process is being restarted. The primary cause of the alarm is that a software problem process has exited abnormally and had to be restarted. If problem is recurrent, contact Cisco TAC. Refer to the [“Obtaining Technical Assistance” section on page xxxviii](#) for detailed instructions on contacting Cisco TAC and opening a service request.

## Process Manager: Going Faulty - Maintenance (26)

The Process Manager: Going Faulty alarm (major) indicates that a PMG process is going faulty. The primary cause of the alarm is that the system has been brought down or the system has detected a fault. If the alarm is not due to the operator intentionally bringing down the system, then the platform has detected a fault and has shut down. This is typically followed by the Maintenance (3) alarm event. To correct the primary cause of the alarm, use the corrective action procedures provided for the Maintenance (3) alarm event. Refer to the [“Local Side has Become Faulty - Maintenance \(3\)” section on page 7-77](#).

## Process Manager: Binary Does not Exist for Process - Maintenance (40)

The Process Manager: Binary Does not Exist for Process alarm (critical) indicates that the platform was not installed correctly. The primary cause of the alarm is that the platform was not installed correctly. To correct the primary cause of the alarm, reinstall the platform.

## Number of Heartbeat Messages Received is Less Than 50% of Expected - Maintenance (42)

The Number of Heartbeat Messages Received is Less Than 50% of Expected alarm (major) indicates that number of HB messages being received is less than 50% of expected number. The primary cause of the alarm is that a network problem has occurred. To correct the primary cause of the alarm, fix the network problem.

## Process Manager: Process Failed to Come Up in Active Mode - Maintenance (43)

The Process Manager: Process Failed to Come Up in Active Mode alarm (critical) indicates that the process has failed to come up in active mode. The primary cause of the alarm is a software or configuration problem. To correct the primary cause of the alarm, restart the platform. If problem persists or is recurrent, contact Cisco TAC. Refer to the [“Obtaining Technical Assistance” section on page xxxviii](#) for detailed instructions on contacting Cisco TAC and opening a service request.

## Process Manager: Process Failed to Come Up in Standby Mode - Maintenance (44)

The Process Manager: Process Failed to Come Up in Standby Mode alarm (critical) indicates that the process has failed to come up in standby mode. The primary cause of the alarm is a software or a configuration problem. To correct the primary cause of the alarm, restart the platform. If problem persists or is recurrent, contact Cisco TAC. Refer to the [“Obtaining Technical Assistance” section on page xxxviii](#) for detailed instructions on contacting Cisco TAC and opening a service request.

## Application Instance State Change Failure - Maintenance (45)

The Application Instance State Change Failure alarm (major) indicates that an application instance state change failed. The primary cause of the alarm is that a switchover of an application instance failed because of a platform fault. To correct the primary cause of the alarm, retry the switchover and if condition continues, contact Cisco TAC. Refer to the [“Obtaining Technical Assistance” section on page xxxviii](#) for detailed instructions on contacting Cisco TAC and opening a service request.

## Thread Watchdog Counter Expired for a Thread - Maintenance (47)

The Thread Watchdog Counter Expired for a Thread alarm (critical) indicates that a thread watchdog counter has expired for a thread. The primary cause of the alarm is a software error. No action is required, the system will automatically recover or shutdown.

## Index Table Usage Exceeded Minor Usage Threshold Level - Maintenance (48)

The Index Table Usage Exceeded Minor Usage Threshold Level alarm (minor) indicates that the IDX table usage has exceeded the minor threshold crossing usage level. The primary cause of the alarm is that call traffic has exceeded design limits. To correct the primary cause of the alarm, verify that traffic is within the rated capacity. The secondary cause of the alarm is that a software problem requiring additional analysis has occurred. To correct the secondary cause of the alarm, contact Cisco TAC. Refer to the [“Obtaining Technical Assistance” section on page xxxviii](#) for detailed instructions on contacting Cisco TAC and opening a service request.

## Index Table Usage Exceeded Major Usage Threshold Level - Maintenance (49)

The Index Table Usage Exceeded Major Usage Threshold Level alarm (major) indicates that the IDX table usage has exceeded the major threshold crossing usage level. The primary cause of the alarm is that call traffic has exceeded design limits. To correct the primary cause of the alarm, verify that traffic is within the rated capacity. The secondary cause of the alarm is that a software problem requiring additional analysis has occurred. To correct the secondary cause of the alarm, contact Cisco TAC. Refer to the [“Obtaining Technical Assistance” section on page xxxviii](#) for detailed instructions on contacting Cisco TAC and opening a service request.

## Index Table Usage Exceeded Critical Usage Threshold Level - Maintenance (50)

The Index Table Usage Exceeded Critical Usage Threshold Level alarm (critical) indicates that the IDX table usage has exceeded the critical threshold crossing usage level. The primary cause of the alarm is that call traffic has exceeded design limits. To correct the primary cause of the alarm, verify that traffic is within the rated capacity. The secondary cause of the alarm is that a software problem requiring additional analysis has occurred. To correct the secondary cause of the alarm, contact Cisco TAC. Refer to the [“Obtaining Technical Assistance” section on page xxxviii](#) for detailed instructions on contacting Cisco TAC and opening a service request.

## A Process Exceeds 70% of Central Processing Unit Usage - Maintenance (51)

The A Process Exceeds 70% of Central Processing Unit Usage alarm (major) indicates that a process has exceeded the CPU usage threshold of 70 percent. The primary cause of the alarm is that a process has entered a state of erratic behavior. To correct the primary cause of the alarm, monitor the process and kill it if necessary.

## The Central Processing Unit Usage is Over 90% Busy - Maintenance (53)

The The Central Processing Unit Usage is Over 90% Busy alarm (critical) indicates that the CPU usage is over the threshold level of 90 percent. The primary causes of the alarm are too numerous to determine. Try to isolate the problem and call Cisco TAC for assistance. Refer to the [“Obtaining Technical Assistance” section on page xxxviii](#) for detailed instructions on contacting Cisco TAC and opening a service request.

## The Five Minute Load Average is Abnormally High - Maintenance (55)

The Five Minute Load Average is Abnormally High alarm (major) indicates the five minute load average is abnormally high. The primary cause of the alarm is that multiple processes are vying for processing time on the system, which is normal in a high traffic situation such as heavy call processing or bulk provisioning. To correct the primary cause of the alarm, monitor the system to ensure all subsystems are performing normally. If so, only lightening the effective load on the system will clear the situation. If not, verify which process(es) are running at abnormally high rates and provide the information to Cisco TAC. Refer to the [“Obtaining Technical Assistance” section on page xxxviii](#) for detailed instructions on contacting Cisco TAC and opening a service request.

## Memory and Swap are Consumed at Critical Levels - Maintenance (57)



### Note

Maintenance (57) is issued by the BTS 10200 system when memory consumption is greater than 95 percent (>95%) and swap space consumption is greater than 50 percent (>50%).

The Memory and Swap are Consumed at Critical Levels alarm (critical) indicates that memory and swap file usage have reached critical levels. The primary cause of the alarm is that a process or multiple processes have consumed a critical amount of memory on the system and the operating system is utilizing a critical amount of the swap space for process execution. This can be a result of high call rates or bulk provisioning activity. To correct the primary cause of the alarm, monitor the system to ensure all subsystems are performing normally. If so, only lightening the effective load on the system will clear the situation. If not, verify which process(es) are running at abnormally high rates and provide the information to Cisco TAC. Refer to the [“Obtaining Technical Assistance” section on page xxxviii](#) for detailed instructions on contacting Cisco TAC and opening a service request.

## No Heartbeat Messages Received Through the Interface - Maintenance (61)

The No Heartbeat Messages Received Through the Interface alarm (critical) indicates that no HB messages are being received through the local network interface. The primary cause of the alarm is that the local network interface is down. To correct the primary cause of the alarm, restore the local network interface. The secondary cause of the alarm is that the mate network interface on the same sub-net is faulty. To correct the secondary cause of the alarm, restore the mate network interface. The tertiary cause of the alarm is network congestion.

## Link Monitor: Interface Lost Communication - Maintenance (62)

The Link Monitor: Interface Lost Communication alarm (major) indicates that a interface has lost communication. The primary cause of the alarm is that the interface cable is pulled out or interface has been set to “down” using ifconfig command. To correct the primary cause of the alarm, restore the network interface. The secondary cause of the alarm is that the interface has no connectivity to any of the machines or routers.

## Outgoing Heartbeat Period Exceeded Limit - Maintenance (63)

The Outgoing Heartbeat Period Exceeded Limit alarm (major) indicates that the outgoing HB period has exceeded the limit. The primary cause of the alarm is system performance degradation due to CPU overload or excessive I/O operations. To correct the primary cause of the alarm, identify the applications which are causing the system degradation via the CLI commands to verify if this is a persistent or on-going situation. Contact Cisco TAC with the gathered information. Refer to the [“Obtaining Technical Assistance” section on page xxxviii](#) for detailed instructions on contacting Cisco TAC and opening a service request.

## Average Outgoing Heartbeat Period Exceeds Major Alarm Limit - Maintenance (64)

The Average Outgoing Heartbeat Period Exceeds Major Alarm Limit alarm (major) indicates that the average outgoing HB period has exceeded the major threshold crossing alarm limit. The primary cause of the alarm is system performance degradation due to CPU overload or excessive I/O operations. To correct the primary cause of the alarm, identify the applications which are causing the system degradation via the CLI commands to verify if this is a persistent or on-going situation. Contact Cisco TAC with the gathered information. Refer to the [“Obtaining Technical Assistance” section on page xxxviii](#) for detailed instructions on contacting Cisco TAC and opening a service request.

## Disk Partition Critically Consumed - Maintenance (65)

The Disk Partition Critically Consumed alarm (critical) indicates that the disk partition consumption has reached critical limits. The primary cause of the alarm is that a process or processes is/are writing extraneous data to the named partition. To correct the primary cause of the alarm, perform a disk clean-up and maintenance on the offending system.

## Disk Partition Significantly Consumed - Maintenance (66)

The Disk Partition Significantly Consumed alarm (major) indicates that the disk partition consumption has reached the major threshold crossing level. The primary cause of the alarm is that a process or processes is/are writing extraneous data to the named partition. To correct the primary cause of the alarm, perform a disk clean-up and maintenance on the offending system.

## The Free Inter-Process Communication Pool Buffers Below Minor Threshold - Maintenance (67)

The The Free Inter-Process Communication Pool Buffers Below Minor Threshold alarm (minor) indicates that the number of free IPC pool buffers has fallen below the minor threshold crossing level. The primary cause of the alarm is that IPC pool buffers are not being freed properly by the application or the application is not able to keep up with the incoming IPC messaging traffic. To correct the primary cause of the alarm, contact Cisco TAC immediately. Refer to the [“Obtaining Technical Assistance” section on page xxxviii](#) for detailed instructions on contacting Cisco TAC and opening a service request.

## The Free Inter-Process Communication Pool Buffers Below Major Threshold - Maintenance (68)

The The Free Inter-Process Communication Pool Buffers Below Major Threshold alarm (major) indicates that the number of free IPC pool buffers has fallen below the major threshold crossing level. The primary cause of the alarm is that IPC pool buffers are not being freed properly by the application or the application is not able to keep up with the incoming IPC messaging traffic. To correct the primary cause of the alarm, contact Cisco TAC immediately. Refer to the [“Obtaining Technical Assistance” section on page xxxviii](#) for detailed instructions on contacting Cisco TAC and opening a service request.

## The Free Inter-Process Communication Pool Buffers Below Critical Threshold - Maintenance (69)

The The Free Inter-Process Communication Pool Buffers Below Critical Threshold alarm (critical) indicates that the number of free IPC pool buffers has fallen below the critical threshold crossing level. The primary cause of the alarm is that IPC pool buffers are not being freed properly by the application or the application is not able to keep up with the incoming IPC messaging traffic. To correct the primary cause of the alarm, contact Cisco TAC immediately. Refer to the [“Obtaining Technical Assistance” section on page xxxviii](#) for detailed instructions on contacting Cisco TAC and opening a service request.

## The Free Inter-Process Communication Pool Buffer Count Below Minimum Required - Maintenance (70)

The The Free Inter-Process Communication Pool Buffer Count Below Minimum Required alarm (critical) indicates that the IPC pool buffers are not being freed properly by the application or the application is not able to keep up with the incoming IPC messaging traffic. The primary cause of the alarm is that IPC pool buffers are not being freed properly by the application or the application is not able to keep up with the incoming IPC messaging traffic. To correct the primary cause of the alarm, contact Cisco TAC immediately. Refer to the [“Obtaining Technical Assistance” section on page xxxviii](#) for detailed instructions on contacting Cisco TAC and opening a service request.

## Local Domain Name System Server Response Too Slow - Maintenance (71)

The Local Domain Name System Server Response Too Slow alarm (major) indicates that the response time of the local DNS server is too slow. The primary cause of the alarm is that the local DNS server is too busy. To correct the primary cause of the alarm, check the local DNS server.

## External Domain Name System Server Response Too Slow - Maintenance (72)

The External Domain Name System Server Response Too Slow alarm (major) indicates that the response time of the external DNS server is too slow. The primary cause of the alarm is that the network traffic level is busy, or the nameserver is very busy. To correct the primary cause of the alarm, check the DNS server(s). The secondary cause of the alarm is that there is a daemon called monitorDNS.sh checking the DNS server every minute or so. It will issue alarm if it cannot contact the DNS server or the response is slow. But it will clear the alarm if later it can contact the DNS server.

## External Domain Name System Server not Responsive - Maintenance (73)

The External Domain Name System Server not Responsive alarm (critical) indicates that the external DNS server is not responding to network queries. The primary cause of the alarm is that the DNS servers or the network may be down. To correct the primary cause of the alarm, check the DNS server(s). The secondary cause of the alarm is that there is a daemon called `monitorDNS.sh` checking DNS server every minute or so. It will issue alarm if it cannot contact the DNS server or the response is slow. But it will clear the alarm if later it can contact the DNS server.

## Local Domain Name System Service not Responsive - Maintenance (74)

The Local Domain Name System Service not Responsive alarm (critical) indicates that the local DNS server is not responding to network queries. The primary cause of the alarm is that the local DNS service may be down. To correct the primary cause of the alarm, check the local DNS server.

## Mate Time Differs Beyond Tolerance - Maintenance (77)

The Mate Time Differs Beyond Tolerance alarm (major) indicates that the mate differs beyond the tolerance. The primary cause of the alarm is that time synchronization not working. To correct the primary cause of the alarm, change the UNIX time on the Faulty or Standby side. If the change is occur on the Standby, stop platform first.

## Average Outgoing Heartbeat Period Exceeds Critical Limit - Maintenance (82)

The Average Outgoing Heartbeat Period Exceeds Critical Limit alarm (critical) indicates that the average outgoing HB period has exceeded the critical limit threshold. The primary cause of the alarm is that the CPU is overloaded. To correct the primary cause of the alarm, shutdown the platform.

## Swap Space Below Minor Threshold - Maintenance (83)

The Swap Space Below Minor Threshold alarm (minor) indicates that the swap space has fallen below the minor threshold level. The primary cause of the alarm is that too many processes are running. To correct the primary cause of the alarm, stop the proliferation of executables (processes-scripts). The secondary cause of the alarm is that the `/tmp` or `/var/run` are being over-used. To correct the secondary cause of the alarm, cleanup the file systems.

## Swap Space Below Major Threshold - Maintenance (84)

The Swap Space Below Major Threshold alarm (major) indicates that the swap space has fallen below the major threshold level. The primary cause of the alarm is that too many processes are running. To correct the primary cause of the alarm, stop the proliferation of executables (processes/shell-procedures). The secondary cause of the alarm is that the `/tmp` or `/var/run` are being over-used. To correct the secondary cause of the alarm, cleanup the file systems.



## Swap Space Below Critical Threshold - Maintenance (85)

The Swap Space Below Critical Threshold alarm (critical) indicates that the swap space has fallen below the critical threshold level. The primary cause of the alarm is that too many processes are running. To correct the primary cause of the alarm, restart the Cisco BTS 10200 Softswitch software or reboot system. The secondary cause of the alarm is that the /tmp or /var/run are being over-used. To correct the secondary cause of the alarm, cleanup the file systems.

## System Health Report Collection Error - Maintenance (86)

The System Health Report Collection Error alarm (minor) indicates that an error occurred while collecting System Health Report. The primary cause of the alarm is that an error occur while collecting the System Health Report. To correct the primary cause of the alarm, contact Cisco TAC. Refer to the [“Obtaining Technical Assistance”](#) section on page xxxviii for detailed instructions on contacting Cisco TAC and opening a service request.

## Status Update Process Request Failed - Maintenance (87)

The Status Update Process Request Failed alarm (major) indicates that the status update process request failed. The primary cause of the alarm is that the “status” command is not working properly. To correct the primary cause of the alarm, verify that the “status” command is working properly via CLI.

## Status Update Process Database List Retrieval Error - Maintenance (88)

The Status Update Process Database List Retrieval Error alarm (major) indicates that the status update process DB had a retrieval error. The primary cause of the alarm is the Oracle DB is not working properly. To correct the primary cause of the alarm, contact Cisco TAC. Refer to the [“Obtaining Technical Assistance”](#) section on page xxxviii for detailed instructions on contacting Cisco TAC and opening a service request.

## Status Update Process Database Update Error - Maintenance (89)

The Status Update Process Database Update Error alarm (major) indicates that the status update process DB had an update error. The primary cause of the alarm is that the MySQL DB on the EMS is not working properly. To correct the primary cause of the alarm, contact Cisco TAC. Refer to the [“Obtaining Technical Assistance”](#) section on page xxxviii for detailed instructions on contacting Cisco TAC and opening a service request.

## Disk Partition Moderately Consumed - Maintenance (90)

The Disk Partition Moderately Consumed alarm (minor) indicates that the disk partition is moderately consumed. The primary cause of the alarm is that a process or processes is/are writing extraneous data to the named partition. To correct the primary cause of the alarm, perform a disk clean-up and maintenance on the offending system.

## Internet Protocol Manager Configuration File Error - Maintenance (91)

The Internet Protocol Manager Configuration File Error alarm (critical) indicates that IPM configuration file has an error. The primary cause of the alarm is a IPM configuration file error. To correct the primary cause of the alarm, check the IPM configuration file (ipm.cfg) for incorrect syntax.

## Internet Protocol Manager Initialization Error - Maintenance (92)

The Internet Protocol Manager Initialization Error alarm (major) indicates that the IPM process failed to initialize correctly. The primary cause of the alarm is that IPM failed to initialize correctly. To correct the primary cause of the alarm, check the “reason” dataword to identify and correct the cause of the alarm.

## Internet Protocol Manager Interface Failure - Maintenance (93)

The Internet Protocol Manager Interface Failure alarm (major) indicates that an IPM interface has failed. The primary cause of the alarm is that IPM failed to create logical interface. To correct the primary cause of the alarm, check the “reason” dataword to identify and correct the cause of the alarm.

## Inter-Process Communication Input Queue Entered Throttle State - Maintenance (97)

The Inter-Process Communication Input Queue Entered Throttle State alarm (critical) alarm indicates that the thread is not able to process its IPC input messages fast enough, hence the input queue has grown too large and is using up too much of the IPC memory pool resource. The primary cause of the alarm is that the indicated thread is not able to process its IPC input messages fast enough, hence the input queue has grown too large and is using up too much of the IPC memory pool resource. To correct the primary cause of the alarm, contact Cisco TAC. Refer to the [“Obtaining Technical Assistance” section on page xxxviii](#) for detailed instructions on contacting Cisco TAC and opening a service request.

## Inter-Process Communication Input Queue Depth at 25% of Its Hi-Watermark - Maintenance (98)

The Inter-Process Communication Input Queue Depth at 25% of Its Hi-Watermark alarm (minor) indicates that the IPC input queue depth has reached 25 percent of its hi-watermark. The primary cause of the alarm is that the indicated thread is not able to process its IPC input messages fast enough, hence the input queue has grown too large and is at 25% of the level at which it will enter the throttle state. To correct the primary cause of the alarm, contact Cisco TAC. Refer to the [“Obtaining Technical Assistance” section on page xxxviii](#) for detailed instructions on contacting Cisco TAC and opening a service request.

## Inter-Process Communication Input Queue Depth at 50% of Its Hi-Watermark - Maintenance (99)

The Inter-Process Communication Input Queue Depth at 50% of Its Hi-Watermark alarm (major) indicates that the IPC input queue depth has reached 50 percent of its hi-watermark. The primary cause of the alarm is that the indicated thread is not able to process its IPC input messages fast enough, hence the input queue has grown too large and is at 50% of the level at which it will enter the throttle state. To correct the primary cause of the alarm, contact Cisco TAC. Refer to the [“Obtaining Technical Assistance” section on page xxxviii](#) for detailed instructions on contacting Cisco TAC and opening a service request.

## Inter-Process Communication Input Queue Depth at 75% of Its Hi-Watermark - Maintenance (100)

The Inter-Process Communication Input Queue Depth at 75% of Its Hi-Watermark alarm (critical) indicates that the IPC input queue depth has reached 75 percent of its hi-watermark. The primary cause of the alarm is that the indicated thread is not able to process its IPC input messages fast enough, hence the input queue has grown too large and is at 75% of the level at which it will enter the throttle state. To correct the primary cause of the alarm, contact Cisco TAC. Refer to the [“Obtaining Technical Assistance” section on page xxxviii](#) for detailed instructions on contacting Cisco TAC and opening a service request.

## Switchover in Progress - Maintenance (101)

The Switchover in Progress alarm (critical) indicates that a system switchover is progress. This alarm is issued when a system switchover is in progress either due to manual switchover (via CLI command), failover switchover, or automatic switchover. No action needs to be taken, the alarm is cleared when switchover is complete. Service is temporarily suspended for a short period of time during this transition. The primary cause of the alarm is that a system switchover occurred either due to manual switchover (via CLI command), failover or automatic switchover. No action need to be taken, the alarm is cleared itself when switchover is complete. The service is temporarily suspended for a short period of time during this transition.

## Thread Watchdog Counter Close to Expiry for a Thread - Maintenance (102)

The Thread Watchdog Counter Close to Expiry for a Thread alarm (critical) indicates that the thread watchdog counter is close to expiry for a thread. The primary cause of the alarm is that a software error has occurred. No further action is required, the Cisco BTS 10200 Softswitch system will automatically recover or shutdown.

## Central Processing Unit is Offline - Maintenance (103)

The Central Processing Unit is Offline alarm (critical) indicates that the CPU is offline. The primary cause of the alarm is operator action. To correct the primary cause of the alarm, restore CPU or contact Cisco TAC. Refer to the [“Obtaining Technical Assistance” section on page xxxviii](#) for detailed instructions on contacting Cisco TAC and opening a service request.





## CHAPTER 8

# Operations Support System Troubleshooting

---

Revised: October 23, 2008, OL-11335-06

## Introduction

This chapter provides the information needed to monitor and troubleshoot Operations Support System events and alarms. This chapter is divided into the following sections:

- [Operations Support System Events and Alarms](#) – Provides a brief overview of each Operations Support System event and alarm.
- [Monitoring Operations Support System Events](#) – Provides the information needed to monitor and correct Operations Support System events.
- [Troubleshooting Operations Support System Alarms](#) – Provides the information needed to troubleshoot and correct Operations Support System alarms.

# Operations Support System Events and Alarms

This section provides a brief overview of the Operations Support System events and alarms for the Cisco BTS 10200 Softswitch in numerical order. [Table 8-1](#) lists all of the Operations Support System events and alarms by severity.



**Note**

Click the Operations Support System message number in [Table 8-1](#) to display information about the event or alarm.

**Table 8-1** Operations Support System (OSS) Events and Alarms by Severity

| CRITICAL | MAJOR                    | MINOR                   | WARNING                  | INFO                    |
|----------|--------------------------|-------------------------|--------------------------|-------------------------|
|          | <a href="#">OSS (2)</a>  | <a href="#">OSS (5)</a> | <a href="#">OSS (7)</a>  | <a href="#">OSS (1)</a> |
|          | <a href="#">OSS (3)</a>  | <a href="#">OSS (8)</a> | <a href="#">OSS (11)</a> |                         |
|          | <a href="#">OSS (4)</a>  | <a href="#">OSS (9)</a> |                          |                         |
|          | <a href="#">OSS (6)</a>  |                         |                          |                         |
|          | <a href="#">OSS (10)</a> |                         |                          |                         |

## OSS (1)

For additional information, refer to the “[Test Report - Operations Support System \(1\)](#)” section on [page 8-9](#).

|             |                    |
|-------------|--------------------|
| DESCRIPTION | Test Report        |
| SEVERITY    | Information (INFO) |
| THRESHOLD   | 10000              |
| THROTTLE    | 0                  |

## OSS (2)

To troubleshoot and correct the cause of the alarm, refer to the [“Undefined Variable in Known Set - Operations Support System \(2\)”](#) section on page 8-12.

|                |                                                                                    |
|----------------|------------------------------------------------------------------------------------|
| DESCRIPTION    | Undefined Variable in Known Set                                                    |
| SEVERITY       | MAJOR                                                                              |
| THRESHOLD      | 100                                                                                |
| THROTTLE       | 0                                                                                  |
| DATAWORDS      | Module Name - STRING [40]<br>Field Name - STRING [40]<br>Field Value - STRING [64] |
| PRIMARY CAUSE  | There was no definition of a data column that could be found in the database.      |
| PRIMARY ACTION | Contact Cisco Technical Assistance Center (TAC) for support.                       |

Refer to the [“Obtaining Technical Assistance”](#) section on page xxxviii for detailed instructions on contacting Cisco TAC and opening a service request.

## OSS (3)

To troubleshoot and correct the cause of the alarm, refer to the [“Undefined Data Column Identification - Operations Support System \(3\)”](#) section on page 8-12.

|                |                                                                                                                                        |
|----------------|----------------------------------------------------------------------------------------------------------------------------------------|
| DESCRIPTION    | Undefined Data Column Identification                                                                                                   |
| SEVERITY       | MAJOR                                                                                                                                  |
| THRESHOLD      | 100                                                                                                                                    |
| THROTTLE       | 0                                                                                                                                      |
| DATAWORDS      | Noun - STRING [40]<br>Data Column ID - STRING [40]                                                                                     |
| PRIMARY CAUSE  | The database does not contain the required data column that was requested via the Simple Network Management Protocol (SNMP) interface. |
| PRIMARY ACTION | Contact Cisco TAC for support.                                                                                                         |

Refer to the [“Obtaining Technical Assistance”](#) section on page xxxviii for detailed instructions on contacting Cisco TAC and opening a service request.

## OSS (4)

To troubleshoot and correct the cause of the alarm, refer to the [“Request Handler Instantiation Error - Operations Support System \(4\)”](#) section on page 8-12.

|                |                                                                                                                             |
|----------------|-----------------------------------------------------------------------------------------------------------------------------|
| DESCRIPTION    | Request Handler Instantiation Error                                                                                         |
| SEVERITY       | MAJOR                                                                                                                       |
| THRESHOLD      | 100                                                                                                                         |
| THROTTLE       | 0                                                                                                                           |
| DATAWORDS      | User Name - STRING [40]<br>Host - STRING [40]<br>Subsystem - STRING [64]                                                    |
| PRIMARY CAUSE  | Resource limitation has prevented the creation of this object. This may come from a lack of memory or a class path problem. |
| PRIMARY ACTION | Contact Cisco TAC for support.                                                                                              |

Refer to the [“Obtaining Technical Assistance”](#) section on page xxxviii for detailed instructions on contacting Cisco TAC and opening a service request.

## OSS (5)

To troubleshoot and correct the cause of the alarm, refer to the [“Structured Query Language Error While Getting Statistics - Operations Support System \(5\)”](#) section on page 8-13.

|                |                                                                                                                                                                     |
|----------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| DESCRIPTION    | Structured Query Language Error While Getting Statistics (SQL Error While Getting Statistics)                                                                       |
| SEVERITY       | MINOR                                                                                                                                                               |
| THRESHOLD      | 100                                                                                                                                                                 |
| THROTTLE       | 0                                                                                                                                                                   |
| DATAWORDS      | Statistics Category - STRING [40]                                                                                                                                   |
| PRIMARY CAUSE  | An error occurred in accessing the Structured Query Language (SQL) database for statistical information in the SNMP subsystem. This may result from a schema error. |
| PRIMARY ACTION | Contact Cisco TAC for support.                                                                                                                                      |

Refer to the [“Obtaining Technical Assistance”](#) section on page xxxviii for detailed instructions on contacting Cisco TAC and opening a service request.



## OSS (6)

To troubleshoot and correct the cause of the alarm, refer to the [“Structured Query Language Connection Error - Operations Support System \(6\)” section on page 8-13](#).

|                |                                                                                                                          |
|----------------|--------------------------------------------------------------------------------------------------------------------------|
| DESCRIPTION    | Structured Query Language Connection Error (SQL Connection Error)                                                        |
| SEVERITY       | MAJOR                                                                                                                    |
| THRESHOLD      | 100                                                                                                                      |
| THROTTLE       | 0                                                                                                                        |
| DATAWORDS      | Error Exception - STRING [64]                                                                                            |
| PRIMARY CAUSE  | The connection to the database timed out or the database server is not running. This is generated in the SNMP subsystem. |
| PRIMARY ACTION | Contact Cisco TAC for support.                                                                                           |

Refer to the [“Obtaining Technical Assistance” section on page xxxviii](#) for detailed instructions on contacting Cisco TAC and opening a service request.

## OSS (7)

To monitor and correct the cause of the event, refer to the [“Simple Network Management Protocol File Read Error - Operations Support System \(7\)” section on page 8-10](#).

|                |                                                                                                    |
|----------------|----------------------------------------------------------------------------------------------------|
| DESCRIPTION    | Simple Network Management Protocol File Read Error (SNMP File Read Error)                          |
| SEVERITY       | WARNING                                                                                            |
| THRESHOLD      | 100                                                                                                |
| THROTTLE       | 0                                                                                                  |
| DATAWORDS      | Filename - STRING [40]                                                                             |
| PRIMARY CAUSE  | The Management Information Base (MIB) file is missing or locked from access by the SNMP subsystem. |
| PRIMARY ACTION | Contact Cisco TAC for support.                                                                     |

Refer to the [“Obtaining Technical Assistance” section on page xxxviii](#) for detailed instructions on contacting Cisco TAC and opening a service request.

## OSS (8)

To troubleshoot and correct the cause of the alarm, refer to the [“No Reply Received from Destination - Operations Support System \(8\)”](#) section on page 8-13.

|                  |                                                                                                                                                                                                                                              |
|------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| DESCRIPTION      | No Reply Received from Destination                                                                                                                                                                                                           |
| SEVERITY         | MINOR                                                                                                                                                                                                                                        |
| THRESHOLD        | 100                                                                                                                                                                                                                                          |
| THROTTLE         | 5                                                                                                                                                                                                                                            |
| DATAWORDS        | JMS Queue Name - STRING [40]                                                                                                                                                                                                                 |
| PRIMARY CAUSE    | Received when there is no response to a command line interface (CLI) command from the Call Agent platform.                                                                                                                                   |
| PRIMARY ACTION   | If this Event Report is issued while the system is stable (i.e. no device failures) and the traffic is at or below the engineered level, then Cisco TAC technical support should be contacted to investigate the cause. (Contact Cisco TAC.) |
| SECONDARY ACTION | If components of the system are in the process of failing or restoring while CLI commands are being issued, then this event report is informational and no further action is required.                                                       |
| TERNARY ACTION   | The traffic measurement reports can be checked to see if there is more traffic being handled than the engineered level. If this is the situation, then the traffic should be reduced or capacity should be added.                            |

Refer to the [“Obtaining Technical Assistance”](#) section on page xxxviii for detailed instructions on contacting Cisco TAC and opening a service request.

## OSS (9)

To troubleshoot and correct the cause of the alarm, refer to the [“Simple Network Management Protocol Authentication Error - Operations Support System \(9\)”](#) section on page 8-13.

|                |                                                                                     |
|----------------|-------------------------------------------------------------------------------------|
| DESCRIPTION    | Simple Network Management Protocol Authentication Error (SNMP Authentication Error) |
| SEVERITY       | MINOR                                                                               |
| THRESHOLD      | 100                                                                                 |
| THROTTLE       | 0                                                                                   |
| DATAWORDS      | RemoteHost - STRING [64]                                                            |
| PRIMARY CAUSE  | Network management system (NMS) issuing wrong community string.                     |
| PRIMARY ACTION | Ensure community string exists via CLI.                                             |

## OSS (10)

To troubleshoot and correct the cause of the alarm, refer to the [“Queue Processing Module Database Management Index Failed with Error - Operations Support System \(10\)”](#) section on page 8-11.

|                  |                                                                                                                                                                                                           |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| DESCRIPTION      | Queue Processing Module Database Management Index Failed with Error (QAM DBM IDX Failed with Error)                                                                                                       |
| SEVERITY         | MAJOR                                                                                                                                                                                                     |
| THRESHOLD        | 50                                                                                                                                                                                                        |
| THROTTLE         | 0                                                                                                                                                                                                         |
| DATAWORDS        | Transaction ID - STRING [32]<br>Sequence Number - EIGHT_BYTES<br>Location Of Error - STRING [16]<br>DBM Result - STRING [64]                                                                              |
| PRIMARY CAUSE    | Queue processing module (QAM) is receiving an error because of Data Mismatch between what is in the database management (DBM) index (IDX) and what is in the Element Management System (EMS) DB (Oracle). |
| PRIMARY ACTION   | View Transaction Queue and execute Audit on the failed table.                                                                                                                                             |
| SECONDARY CAUSE  | DBM IDX is failing when attempting to perform SQL command.                                                                                                                                                |
| SECONDARY ACTION | Contact Cisco Support.                                                                                                                                                                                    |

Refer to the [“Obtaining Technical Assistance”](#) section on page xxxviii for detailed instructions on contacting Cisco TAC and opening a service request.

## OSS (11)

To monitor and correct the cause of the event, refer to the [“Queue Processing Module Database Management Index Mismatch During Add or Delete - Operations Support System \(11\)”](#) section on page 8-11.

|                |                                                                                                                                           |
|----------------|-------------------------------------------------------------------------------------------------------------------------------------------|
| DESCRIPTION    | Queue Processing Module Database Management Index Mismatch During Add or Delete (QAM DBM IDX mismatch during Add or Delete)               |
| SEVERITY       | WARNING                                                                                                                                   |
| THRESHOLD      | 100                                                                                                                                       |
| THROTTLE       | 0                                                                                                                                         |
| DATAWORDS      | Transaction ID - STRING [32]<br>Sequence Number - EIGHT_BYTES<br>Location Of Error - STRING [16]<br>DBM Result - STRING [64]              |
| PRIMARY CAUSE  | QAM is received a warning that either an entry already exists in DBM IDX during Add or an entry is nonexistent during a Delete operation. |
| PRIMARY ACTION | None needed.                                                                                                                              |

# Monitoring Operations Support System Events

This section provides the information needed to monitor and correct Operations Support System events. [Table 8-2](#) lists all Operations Support System events in numerical order and provides cross reference to each subsection in this section.

**Table 8-2** Cisco BTS 10200 Softswitch OSS Events

| Event Type | Event Name                                                                                                                       | Event Severity |
|------------|----------------------------------------------------------------------------------------------------------------------------------|----------------|
| OSS(1)     | <a href="#">Test Report - Operations Support System (1)</a>                                                                      | INFO           |
| OSS(2)     | <a href="#">Undefined Variable in Known Set - Operations Support System (2)</a>                                                  | MAJOR          |
| OSS(3)     | <a href="#">Undefined Data Column Identification - Operations Support System (3)</a>                                             | MAJOR          |
| OSS(4)     | <a href="#">Request Handler Instantiation Error - Operations Support System (4)</a>                                              | MAJOR          |
| OSS(5)     | <a href="#">Structured Query Language Error While Getting Statistics - Operations Support System (5)</a>                         | MINOR          |
| OSS(6)     | <a href="#">Structured Query Language Connection Error - Operations Support System (6)</a>                                       | MAJOR          |
| OSS(7)     | <a href="#">Simple Network Management Protocol File Read Error - Operations Support System (7)</a>                               | WARNING        |
| OSS(8)     | <a href="#">No Reply Received from Destination - Operations Support System (8)</a>                                               | MINOR          |
| OSS(9)     | <a href="#">Simple Network Management Protocol Authentication Error - Operations Support System (9)</a>                          | MINOR          |
| OSS(10)    | <a href="#">Queue Processing Module Database Management Index Failed with Error - Operations Support System (10)</a>             | MAJOR          |
| OSS(11)    | <a href="#">Queue Processing Module Database Management Index Mismatch During Add or Delete - Operations Support System (11)</a> | WARNING        |

## Test Report - Operations Support System (1)

The Test Report event is for testing the operations support system event category. The event is informational and no further action is required.

## Undefined Variable in Known Set - Operations Support System (2)

The Undefined Variable in Known Set alarm (major) indicates that there was not a definition for a data column that could be found in the database. To troubleshoot and correct the cause of the Undefined Variable in Known Set alarm, refer to the [“Undefined Variable in Known Set - Operations Support System \(2\)”](#) section on page 8-12.

## Undefined Data Column Identification - Operations Support System (3)

The Undefined Data Column Identification alarm (major) indicates that the database does not contain the required data column that was requested via the SNMP interface. To troubleshoot and correct the cause of the Undefined Data Column Identification alarm, refer to the [“Undefined Data Column Identification - Operations Support System \(3\)”](#) section on page 8-12.

## Request Handler Instantiation Error - Operations Support System (4)

The Request Handler Instantiation Error alarm (major) indicates that the creation of the request handler object has failed. To troubleshoot and correct the cause of the Request Handler Instantiation Error alarm, refer to [“Request Handler Instantiation Error - Operations Support System \(4\)” section on page 8-12.](#)

## Structured Query Language Error While Getting Statistics - Operations Support System (5)

The Structured Query Language Error While Getting Statistics alarm (minor) indicates that an error occurred while accessing the SQL database for statistical information in the SNMP subsystem. To troubleshoot and correct the cause of the Structured Query Language Error While Getting Statistics alarm, refer to the [“Structured Query Language Error While Getting Statistics - Operations Support System \(5\)” section on page 8-13.](#)

## Structured Query Language Connection Error - Operations Support System (6)

The Structured Query Language Connection Error alarm (major) indicates that the connection to the database timed out or the database server is not running. To troubleshoot and correct the cause of the Structured Query Language Connection Error alarm, refer to the [“Structured Query Language Connection Error - Operations Support System \(6\)” section on page 8-13.](#)

## Simple Network Management Protocol File Read Error - Operations Support System (7)

The Simple Network Management Protocol File Read Error event serves as a warning that the requested MIB file is missing or locked from access by the SNMP subsystem. To correct the primary cause of the event, contact Cisco TAC. Refer to the [“Obtaining Technical Assistance” section on page xxxviii](#) for detailed instructions on contacting Cisco TAC and opening a service request.

## No Reply Received from Destination - Operations Support System (8)

The No Reply Received from Destination alarm (minor) indicates that there no reply received from the destination. To troubleshoot and correct the cause of the No Reply Received from Destination alarm, refer to the [“No Reply Received from Destination - Operations Support System \(8\)” section on page 8-13.](#)

## Simple Network Management Protocol Authentication Error - Operations Support System (9)

The Simple Network Management Protocol Authentication Error alarm (minor) indicates that the NMS is issuing the wrong community string. To troubleshoot and correct the cause of the Simple Network Management Protocol Authentication Error alarm, refer to the [“Simple Network Management Protocol Authentication Error - Operations Support System \(9\)” section on page 8-13.](#)

## Queue Processing Module Database Management Index Failed with Error - Operations Support System (10)

The Queue Processing Module Database Management Index Failed with Error alarm (major) indicates that the QAM is receiving an error because of a data mismatch between the information that is in the DBM IDX and the information that is in the EMS database (Oracle). To troubleshoot and correct the cause of the Queue Processing Module Database Management Index Failed with Error alarm, refer to the [“Queue Processing Module Database Management Index Failed with Error - Operations Support System \(10\)”](#) section on page 8-14.

## Queue Processing Module Database Management Index Mismatch During Add or Delete - Operations Support System (11)

The Queue Processing Module Database Management Index Mismatch During Add or Delete event serves as a warning that the QAM has received a warning that either an entry already exists in DBM IDX during an Add operation or an entry is nonexistent during a Delete operation. No further action is required.

# Troubleshooting Operations Support System Alarms

This section provides the information needed to monitor and correct Operations Support System alarms. [Table 8-3](#) lists all Operations Support System alarms in numerical order and provides cross reference to each subsection in this section.

**Table 8-3** Cisco BTS 10200 Softswitch OSS Alarms

| Alarm Type | Alarm Name                                                                                           | Alarm Severity |
|------------|------------------------------------------------------------------------------------------------------|----------------|
| OSS(2)     | Undefined Variable in Known Set - Operations Support System (2)                                      | MAJOR          |
| OSS(3)     | Undefined Data Column Identification - Operations Support System (3)                                 | MAJOR          |
| OSS(4)     | Request Handler Instantiation Error - Operations Support System (4)                                  | MAJOR          |
| OSS(5)     | Structured Query Language Error While Getting Statistics - Operations Support System (5)             | MINOR          |
| OSS(6)     | Structured Query Language Connection Error - Operations Support System (6)                           | MAJOR          |
| OSS(8)     | No Reply Received from Destination - Operations Support System (8)                                   | MINOR          |
| OSS(9)     | Simple Network Management Protocol Authentication Error - Operations Support System (9)              | MINOR          |
| OSS(10)    | Queue Processing Module Database Management Index Failed with Error - Operations Support System (10) | MAJOR          |

## Undefined Variable in Known Set - Operations Support System (2)

The Undefined Variable in Known Set alarm (major) indicates that there was not a definition for a data column that could be found in the database. The primary cause of the alarm is that there was no definition of a data column that could be found in the database. To correct the primary cause of the alarm, contact Cisco TAC for support. Refer to the [“Obtaining Technical Assistance”](#) section on page xxxviii for detailed instructions on contacting Cisco TAC and opening a service request.

## Undefined Data Column Identification - Operations Support System (3)

The Undefined Data Column Identification alarm (major) indicates that the database does not contain the required data column that was requested via the SNMP interface. The primary cause of the alarm is that the database does not contain the required data column that was requested via the SNMP interface. To correct the primary cause of the alarm, contact Cisco TAC for support. Refer to the [“Obtaining Technical Assistance”](#) section on page xxxviii for detailed instructions on contacting Cisco TAC and opening a service request.

## Request Handler Instantiation Error - Operations Support System (4)

The Request Handler Instantiation Error alarm (major) indicates that the creation of the request handler object has failed. The primary cause of the alarm is that a resource limitation has prevented the creation of this object. A lack of memory or a Class Path problem may cause the alarm. To correct the primary cause of the alarm, contact Cisco TAC for support. Refer to the [“Obtaining Technical Assistance”](#) section on page xxxviii for detailed instructions on contacting Cisco TAC and opening a service request.



## Structured Query Language Error While Getting Statistics - Operations Support System (5)

The Structured Query Language Error While Getting Statistics alarm (minor) indicates that an error occurred while accessing the SQL database for statistical information in the SNMP subsystem. The primary cause of the alarm is that an error occurred in accessing the SQL database for statistical information in the SNMP subsystem. The alarm may result from schema error. To correct the primary cause of the alarm, contact Cisco TAC for support. Refer to the [“Obtaining Technical Assistance” section on page xxxviii](#) for detailed instructions on contacting Cisco TAC and opening a service request.

## Structured Query Language Connection Error - Operations Support System (6)

The Structured Query Language Connection Error alarm (major) indicates that the connection to the database timed out or the database server is not running. The primary cause of the alarm is that the connection to the database timed out or the database server is not running. The alarm is generated in the SNMP subsystem. To correct the primary cause of the alarm, contact Cisco TAC for support. Refer to the [“Obtaining Technical Assistance” section on page xxxviii](#) for detailed instructions on contacting Cisco TAC and opening a service request.

## No Reply Received from Destination - Operations Support System (8)

The No Reply Received from Destination alarm (minor) indicates that there no reply received from the destination. The alarm is received when there is no response to a CLI command from the Call Agent platform. If this alarm is issued while the system is stable (i.e. no device failures) and the traffic is at or below the engineered level, then Cisco TAC technical support should be contacted to investigate the cause. If components of the system are in the process of failing or restoring while CLI commands are being issued, then this alarm is informational and no further action is required. The traffic measurement reports can be checked to see if there is more traffic being handled than the engineered level. If this is the situation, then the traffic should be reduced or capacity should be added. Refer to the [“Obtaining Technical Assistance” section on page xxxviii](#) for detailed instructions on contacting Cisco TAC and opening a service request.

## Simple Network Management Protocol Authentication Error - Operations Support System (9)

The Simple Network Management Protocol Authentication Error alarm (minor) indicates that the NMS is issuing the wrong community string. The primary cause of the alarm is that the NMS issuing the wrong community string. To correct the primary cause of the alarm, ensure the correct community string exists via CLI.

## Queue Processing Module Database Management Index Failed with Error - Operations Support System (10)

The Queue Processing Module Database Management Index Failed with Error alarm (major) indicates that the QAM is receiving an error because of a data mismatch between the information that is in DBM IDX and the information that is in the EMS database (Oracle). The primary cause of the alarm is that the QAM is receiving an error because of a data mismatch between what is in the DBM IDX and what is in the EMS db (oracle). To correct the primary cause of the alarm, view the Transaction Queue and execute an Audit on the failed table. The secondary cause of the alarm is that the DBM IDX is failing when attempting to perform a SQL command. To correct the secondary cause of the alarm, contact Cisco TAC. Refer to the [“Obtaining Technical Assistance” section on page xxxviii](#) for detailed instructions on contacting Cisco TAC and opening a service request.



## CHAPTER 9

# Security Troubleshooting

---

Revised: October 23, 2008, OL-11335-06

## Introduction

This chapter provides the information needed to monitor and troubleshoot Security events and alarms. This chapter is divided into the following sections:

- [Security Events and Alarms](#) – Provides a brief overview of each Security event and alarm.
- [Monitoring Security Events](#) – Provides the information needed to monitor and correct Security events.
- [Troubleshooting Security Alarms](#) – Provides the information needed to troubleshoot and correct Security alarms.

# Security Events and Alarms

This section provides a brief overview of the Security events and alarms for the Cisco BTS 10200 Softswitch in numerical order. [Table 9-1](#) lists all of the Security events and alarms by severity.



**Note**

Click the Security message number in [Table 9-1](#) to display information about the event or alarm.

**Table 9-1 Security Events and Alarms by Severity**

| CRITICAL | MAJOR                        | MINOR | WARNING                      | INFO                         |
|----------|------------------------------|-------|------------------------------|------------------------------|
|          | <a href="#">SECURITY (3)</a> |       | <a href="#">SECURITY (2)</a> | <a href="#">SECURITY (1)</a> |
|          |                              |       | <a href="#">SECURITY (4)</a> |                              |
|          |                              |       | <a href="#">SECURITY (5)</a> |                              |

## SECURITY (1)

For additional information, refer to the [“Test Report - Security \(1\)”](#) section on page 9-5.

|             |                    |
|-------------|--------------------|
| DESCRIPTION | Test Report        |
| SEVERITY    | Information (INFO) |
| THRESHOLD   | 100                |
| THROTTLE    | 0                  |

## SECURITY (2)

To monitor and correct the cause of the event, refer to the [“Invalid Credentials Presented by a Session Initiation Protocol Phone - Security \(2\)”](#) section on page 9-5.

|                |                                                                                                                               |
|----------------|-------------------------------------------------------------------------------------------------------------------------------|
| DESCRIPTION    | Invalid Credentials Presented by a Session Initiation Protocol Phone (Invalid Credentials Presented by a SIP Phone)           |
| SEVERITY       | WARNING                                                                                                                       |
| THRESHOLD      | 100                                                                                                                           |
| THROTTLE       | 0                                                                                                                             |
| DATAWORDS      | Authentication User Name - STRING [33]<br>From AOR - STRING [65]<br>SIP Request Type - STRING [15]<br>Sender IP - STRING [20] |
| PRIMARY CAUSE  | Invalid credentials in Session Initiation Protocol (SIP) request.                                                             |
| PRIMARY ACTION | Ensure password on SIP phone matches value provisioned in Cisco BTS 10200 Softswitch.                                         |

## SECURITY (3)

To troubleshoot and correct the cause of the alarm, refer to the [“Internet Protocol Security Connection Down - Security \(3\)” section on page 9-7](#).

|                |                                                                                                                                                                                                            |
|----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| DESCRIPTION    | Internet Protocol Security Connection Down (IPSEC Connection Down)                                                                                                                                         |
| SEVERITY       | MAJOR                                                                                                                                                                                                      |
| THRESHOLD      | 100                                                                                                                                                                                                        |
| THROTTLE       | 0                                                                                                                                                                                                          |
| PRIMARY CAUSE  | Kerberized management server (KMS) fails to establish the pf_key socket with the Internet Protocol security (IPSEC) engine. Implies that the IPSEC engine is not running and that it may not be installed. |
| PRIMARY ACTION | 1. Verify that IPSEC is installed and running in the kernel.<br>2. Reboot.<br>3. If problem persists, call the Technical Assistance Center (TAC). (Contact Cisco TAC.)                                     |

Refer to the [“Obtaining Technical Assistance” section on page xxxviii](#) for detailed instructions on contacting Cisco TAC and opening a service request.

## SECURITY (4)

To monitor and correct the cause of the event, refer to the [“Internet Protocol Security Media Terminal Adapter Key Establish Error - Security \(4\)” section on page 9-5](#).

|                |                                                                                                                       |
|----------------|-----------------------------------------------------------------------------------------------------------------------|
| DESCRIPTION    | Internet Protocol Security Media Terminal Adapter Key Establish Error (IPSEC MTA Key Establish Error)                 |
| SEVERITY       | WARNING                                                                                                               |
| THRESHOLD      | 100                                                                                                                   |
| THROTTLE       | 0                                                                                                                     |
| PRIMARY CAUSE  | Failure to establish the IPSEC keys to a given media terminal adapter (MTA) using Kerberized key management protocol. |
| PRIMARY ACTION | Validate kerberos and mta device provisioning.                                                                        |

## SECURITY (5)

To monitor and correct the cause of the event, refer to the [“Internet Protocol Security Outgoing Security Association Not Found - Security \(5\)”](#) section on page 9-6.

|                |                                                                                                                                                  |
|----------------|--------------------------------------------------------------------------------------------------------------------------------------------------|
| DESCRIPTION    | Internet Protocol Security Outgoing Security Association Not Found (IPSEC Outgoing SA Not Found)                                                 |
| SEVERITY       | WARNING                                                                                                                                          |
| THRESHOLD      | 100                                                                                                                                              |
| THROTTLE       | 0                                                                                                                                                |
| PRIMARY CAUSE  | KMS receives SA-missing msgs from the IPSEC engine and is unable to find a provisioned device to establish the needed security association (SA). |
| PRIMARY ACTION | Remove or modify the security policy which caused the “SA not found” error. Assumes that security is provisioned.                                |

# Monitoring Security Events

This section provides the information needed to monitor and correct Security events. [Table 9-2](#) lists all Security events in numerical order and provides cross reference to each subsection in this section.

**Table 9-2** Cisco BTS 10200 Softswitch Security Events

| Event Type  | Event Name                                                                                           | Event Severity |
|-------------|------------------------------------------------------------------------------------------------------|----------------|
| SECURITY(1) | <a href="#">Test Report - Security (1)</a>                                                           | INFO           |
| SECURITY(2) | <a href="#">Invalid Credentials Presented by a Session Initiation Protocol Phone - Security (2)</a>  | WARNING        |
| SECURITY(3) | <a href="#">Internet Protocol Security Connection Down - Security (3)</a>                            | MAJOR          |
| SECURITY(4) | <a href="#">Internet Protocol Security Media Terminal Adapter Key Establish Error - Security (4)</a> | WARNING        |
| SECURITY(5) | <a href="#">Internet Protocol Security Outgoing Security Association Not Found - Security (5)</a>    | WARNING        |

## Test Report - Security (1)

The Test Report event is for testing the security event category. The event is informational and no further action is required.

## Invalid Credentials Presented by a Session Initiation Protocol Phone - Security (2)

The Invalid Credentials Presented by a Session Initiation Protocol Phone event serves as a warning that credentials in a SIP request are not valid. To correct the cause of the event, ensure that password provisioned on the SIP phone matches the value provisioned in the Cisco BTS 10200 Softswitch.

## Internet Protocol Security Connection Down - Security (3)

The Internet Protocol Security Connection Down alarm (major) indicates that the IP security engine is not running. To troubleshoot and correct the cause of the Internet Protocol Security Connection Down alarm, refer to the [“Internet Protocol Security Connection Down - Security \(3\)”](#) section on page 9-7.

## Internet Protocol Security Media Terminal Adapter Key Establish Error - Security (4)

The Internet Protocol Security Media Terminal Adapter Key Establish Error event serves as a warning that the IPSEC MTA key establishment failed. The primary cause of the event is that a failure to establish the IPSEC keys to a given MTA using Kerberized key management protocol occurred. To correct the primary cause of the event, validate Kerberos provisioning and MTA device provisioning.

## Internet Protocol Security Outgoing Security Association Not Found - Security (5)

The Internet Protocol Security Outgoing Security Association Not Found event serves as a warning that the KMS is unable to find a provisioned device to establish the needed SA. To correct the primary cause of the event, remove or modify the security policy which caused the 'SA not found' error.



# Troubleshooting Security Alarms

This section provides the information needed to monitor and correct Security alarms. [Table 9-3](#) lists all Security alarms in numerical order and provides cross reference to each subsection in this section.

**Table 9-3** *Cisco BTS 10200 Softswitch Security Alarms*

| Alarm Type  | Alarm Name                                                                | Alarm Severity |
|-------------|---------------------------------------------------------------------------|----------------|
| SECURITY(3) | <a href="#">Internet Protocol Security Connection Down - Security (3)</a> | MAJOR          |

## Internet Protocol Security Connection Down - Security (3)

The Internet Protocol Security Connection Down alarm (major) indicates that the IP security engine is not running. The primary cause of the alarm is that the KMS has failed to establish the pf\_key socket with the IPSEC engine. The alarm implies that the IPSEC engine is not running and that it may not be installed. To primary cause of the alarm, verify that IPSEC is installed and running in the kernel and reboot the platform. If problem persists or is recurrent, contact Cisco TAC. Refer to the [“Obtaining Technical Assistance” section on page xxxviii](#) for detailed instructions on contacting Cisco TAC and opening a service request.





# CHAPTER 10

## Signaling Troubleshooting

---

Revised: October 23, 2008, OL-11335-06

### Introduction

This chapter provides the information needed to monitor and troubleshoot Signaling events and alarms. This chapter is divided into the following sections:

- [Signaling Events and Alarms](#) – Provides a brief overview of each Signaling event and alarm.
- [Monitoring Signaling Events](#) – Provides the information needed to monitor and correct Signaling events.
- [Troubleshooting Signaling Alarms](#) – Provides the information needed to troubleshoot and correct Signaling alarms.



#### Caution

The use of the UNIX **ifconfig down** command on any signaling interface to test or troubleshoot network or interface failures of the Cisco BTS 10200 Softswitch Signaling Interface may lead to undesirable consequences or conditions.

---



#### Note

The following billing records are created when a call is rejected due to overload conditions:

- SS7 termination cause code 42
  - Cable signaling stop event cause code “resource unavailable”
- Calls rejected by the signaling adapter will not generate a billing record.
-

# Signaling Events and Alarms

This section provides a brief overview of the Signaling events and alarms for the Cisco BTS 10200 Softswitch in numerical order. [Table 10-1](#) lists all signaling events and alarms by severity.



**Note**

Click the Signaling message number in [Table 10-1](#) to display information about the event or alarm.

**Table 10-1**      *Signaling Events and Alarms by Severity*

| CRITICAL                        | MAJOR                           | MINOR                           | WARNING                         | INFO                            |
|---------------------------------|---------------------------------|---------------------------------|---------------------------------|---------------------------------|
| <a href="#">SIGNALING (12)</a>  | <a href="#">SIGNALING (7)</a>   | <a href="#">SIGNALING (10)</a>  | <a href="#">SIGNALING (2)</a>   | <a href="#">SIGNALING (1)</a>   |
| <a href="#">SIGNALING (64)</a>  | <a href="#">SIGNALING (8)</a>   | <a href="#">SIGNALING (14)</a>  | <a href="#">SIGNALING (3)</a>   | <a href="#">SIGNALING (42)</a>  |
| <a href="#">SIGNALING (65)</a>  | <a href="#">SIGNALING (9)</a>   | <a href="#">SIGNALING (15)</a>  | <a href="#">SIGNALING (4)</a>   | <a href="#">SIGNALING (43)</a>  |
| <a href="#">SIGNALING (69)</a>  | <a href="#">SIGNALING (11)</a>  | <a href="#">SIGNALING (16)</a>  | <a href="#">SIGNALING (6)</a>   | <a href="#">SIGNALING (44)</a>  |
| <a href="#">SIGNALING (75)</a>  | <a href="#">SIGNALING (13)</a>  | <a href="#">SIGNALING (17)</a>  | <a href="#">SIGNALING (25)</a>  | <a href="#">SIGNALING (45)</a>  |
| <a href="#">SIGNALING (80)</a>  | <a href="#">SIGNALING (19)</a>  | <a href="#">SIGNALING (18)</a>  | <a href="#">SIGNALING (26)</a>  | <a href="#">SIGNALING (46)</a>  |
| <a href="#">SIGNALING (81)</a>  | <a href="#">SIGNALING (20)</a>  | <a href="#">SIGNALING (22)</a>  | <a href="#">SIGNALING (27)</a>  | <a href="#">SIGNALING (49)</a>  |
| <a href="#">SIGNALING (82)</a>  | <a href="#">SIGNALING (21)</a>  | <a href="#">SIGNALING (24)</a>  | <a href="#">SIGNALING (28)</a>  | <a href="#">SIGNALING (50)</a>  |
| <a href="#">SIGNALING (83)</a>  | <a href="#">SIGNALING (23)</a>  | <a href="#">SIGNALING (36)</a>  | <a href="#">SIGNALING (29)</a>  | <a href="#">SIGNALING (51)</a>  |
| <a href="#">SIGNALING (84)</a>  | <a href="#">SIGNALING (40)</a>  | <a href="#">SIGNALING (78)</a>  | <a href="#">SIGNALING (30)</a>  | <a href="#">SIGNALING (52)</a>  |
| <a href="#">SIGNALING (85)</a>  | <a href="#">SIGNALING (59)</a>  | <a href="#">SIGNALING (92)</a>  | <a href="#">SIGNALING (31)</a>  | <a href="#">SIGNALING (53)</a>  |
| <a href="#">SIGNALING (107)</a> | <a href="#">SIGNALING (63)</a>  | <a href="#">SIGNALING (93)</a>  | <a href="#">SIGNALING (32)</a>  | <a href="#">SIGNALING (54)</a>  |
| <a href="#">SIGNALING (110)</a> | <a href="#">SIGNALING (66)</a>  | <a href="#">SIGNALING (94)</a>  | <a href="#">SIGNALING (33)</a>  | <a href="#">SIGNALING (55)</a>  |
| <a href="#">SIGNALING (119)</a> | <a href="#">SIGNALING (68)</a>  | <a href="#">SIGNALING (95)</a>  | <a href="#">SIGNALING (34)</a>  | <a href="#">SIGNALING (57)</a>  |
| <a href="#">SIGNALING (120)</a> | <a href="#">SIGNALING (79)</a>  | <a href="#">SIGNALING (96)</a>  | <a href="#">SIGNALING (60)</a>  | <a href="#">SIGNALING (58)</a>  |
| <a href="#">SIGNALING (142)</a> | <a href="#">SIGNALING (86)</a>  | <a href="#">SIGNALING (97)</a>  | <a href="#">SIGNALING (70)</a>  | <a href="#">SIGNALING (61)</a>  |
| <a href="#">SIGNALING (144)</a> | <a href="#">SIGNALING (87)</a>  | <a href="#">SIGNALING (98)</a>  | <a href="#">SIGNALING (71)</a>  | <a href="#">SIGNALING (62)</a>  |
|                                 | <a href="#">SIGNALING (88)</a>  | <a href="#">SIGNALING (99)</a>  | <a href="#">SIGNALING (72)</a>  | <a href="#">SIGNALING (76)</a>  |
|                                 | <a href="#">SIGNALING (89)</a>  | <a href="#">SIGNALING (100)</a> | <a href="#">SIGNALING (73)</a>  | <a href="#">SIGNALING (77)</a>  |
|                                 | <a href="#">SIGNALING (90)</a>  | <a href="#">SIGNALING (101)</a> | <a href="#">SIGNALING (74)</a>  | <a href="#">SIGNALING (104)</a> |
|                                 | <a href="#">SIGNALING (91)</a>  | <a href="#">SIGNALING (102)</a> | <a href="#">SIGNALING (115)</a> | <a href="#">SIGNALING (105)</a> |
|                                 | <a href="#">SIGNALING (103)</a> | <a href="#">SIGNALING (106)</a> | <a href="#">SIGNALING (132)</a> | <a href="#">SIGNALING (133)</a> |
|                                 | <a href="#">SIGNALING (108)</a> | <a href="#">SIGNALING (112)</a> | <a href="#">SIGNALING (138)</a> | <a href="#">SIGNALING (134)</a> |
|                                 | <a href="#">SIGNALING (109)</a> | <a href="#">SIGNALING (117)</a> | <a href="#">SIGNALING (141)</a> | <a href="#">SIGNALING (135)</a> |
|                                 | <a href="#">SIGNALING (111)</a> | <a href="#">SIGNALING (118)</a> |                                 | <a href="#">SIGNALING (136)</a> |
|                                 | <a href="#">SIGNALING (113)</a> | <a href="#">SIGNALING (124)</a> |                                 | <a href="#">SIGNALING (137)</a> |
|                                 | <a href="#">SIGNALING (114)</a> | <a href="#">SIGNALING (143)</a> |                                 | <a href="#">SIGNALING (139)</a> |
|                                 | <a href="#">SIGNALING (116)</a> | <a href="#">SIGNALING (145)</a> |                                 | <a href="#">SIGNALING (140)</a> |
|                                 | <a href="#">SIGNALING (121)</a> | <a href="#">SIGNALING (150)</a> |                                 |                                 |

**Table 10-1**      **Signaling Events and Alarms by Severity (continued)**

| CRITICAL | MAJOR                           | MINOR | WARNING | INFO |
|----------|---------------------------------|-------|---------|------|
|          | <a href="#">SIGNALING (122)</a> |       |         |      |
|          | <a href="#">SIGNALING (125)</a> |       |         |      |
|          | <a href="#">SIGNALING (126)</a> |       |         |      |
|          | <a href="#">SIGNALING (127)</a> |       |         |      |

## SIGNALING (1)

For additional information, refer to the [“Test Report - Signaling \(1\)”](#) section on page 10-79.

|             |                    |
|-------------|--------------------|
| DESCRIPTION | Test Report        |
| SEVERITY    | Information (INFO) |
| THRESHOLD   | 10000              |
| THROTTLE    | 0                  |

## SIGNALING (2)

To monitor and correct the cause of the event, refer to the [“Message Encoding Error - Signaling \(2\)”](#) section on page 10-80.

|                  |                                                                                                                                                                                                                    |
|------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| DESCRIPTION      | Message Encoding Error                                                                                                                                                                                             |
| SEVERITY         | WARNING                                                                                                                                                                                                            |
| THRESHOLD        | 100                                                                                                                                                                                                                |
| THROTTLE         | 0                                                                                                                                                                                                                  |
| DATAWORDS        | Endpoint Name - STRING [40]<br>Message Type - STRING [40]<br>Gateway Type - STRING [32]                                                                                                                            |
| PRIMARY CAUSE    | Issued when there is a message encoding error on sending an MGCP message.                                                                                                                                          |
| PRIMARY ACTION   | If this Error Report is issued while doing interoperability testing with a gateway using MGCP, then capture the MGCP message flow and forward it to Cisco TAC technical support for analysis. (Contact Cisco TAC.) |
| SECONDARY ACTION | When an unexpected MGCP message occurs, call Cisco TAC technical support to identify the root cause. (Contact Cisco TAC.)                                                                                          |

Refer to the [“Obtaining Technical Assistance”](#) section on page xxxviii for detailed instructions on contacting Cisco TAC and opening a service request.

## SIGNALING (3)

To monitor and correct the cause of the event, refer to the [“Message Decoding Error - Signaling \(3\)” section on page 10-80](#).

|                  |                                                                                                                                                                                                                    |
|------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| DESCRIPTION      | Message Decoding Error                                                                                                                                                                                             |
| SEVERITY         | WARNING                                                                                                                                                                                                            |
| THRESHOLD        | 100                                                                                                                                                                                                                |
| THROTTLE         | 0                                                                                                                                                                                                                  |
| DATAWORDS        | Endpoint Name - STRING [40]<br>Gateway Type - STRING [40]<br>Message Type - STRING [40]                                                                                                                            |
| PRIMARY CAUSE    | Issued when there is a message decoding error on receiving an MGCP message.                                                                                                                                        |
| PRIMARY ACTION   | If this Error Report is issued while doing interoperability testing with a gateway using MGCP, then capture the MGCP message flow and forward it to Cisco TAC technical support for analysis. (Contact Cisco TAC.) |
| SECONDARY ACTION | When an unexpected MGCP message occurs, call Cisco TAC technical support to identify the root cause. (Contact Cisco TAC.)                                                                                          |

Refer to the [“Obtaining Technical Assistance” section on page xxxviii](#) for detailed instructions on contacting Cisco TAC and opening a service request.

## SIGNALING (4)

To monitor and correct the cause of the event, refer to the [“Invalid Message Received - Signaling \(4\)” section on page 10-80](#).

|                   |                                                                                                                                       |
|-------------------|---------------------------------------------------------------------------------------------------------------------------------------|
| DESCRIPTION       | Invalid Message Received                                                                                                              |
| SEVERITY          | WARNING                                                                                                                               |
| THRESHOLD         | 100                                                                                                                                   |
| THROTTLE          | 0                                                                                                                                     |
| DATAWORDS         | Endpoint Name - STRING [40]<br>Message Type - STRING [40]                                                                             |
| PRIMARY CAUSE     | Issued when a signaling adapter has received an invalid message from the specified endpoint.                                          |
| PRIMARY ACTION    | Monitor the associated signaling link to see if there is an interruption of service on the link.                                      |
| SECONDARY ACTION  | If there is a communication problem, restart the link.                                                                                |
| TERNARY ACTION    | Verify that the version of the protocol used by the device at the endpoint is consistent with the version expected by the call agent. |
| SUBSEQUENT ACTION | If there is a mismatch, then either the endpoint or call agent must be re-provisioned.                                                |

**Note**

SIGNALING (5) is not used.

## SIGNALING (6)

To monitor and correct the cause of the event, refer to the [“Database Module Function Call Failure - Signaling \(6\)”](#) section on page 10-80.

|                  |                                                                                                                                                                 |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| DESCRIPTION      | Database Module Function Call Failure                                                                                                                           |
| SEVERITY         | WARNING                                                                                                                                                         |
| THRESHOLD        | 100                                                                                                                                                             |
| THROTTLE         | 0                                                                                                                                                               |
| DATAWORDS        | Endpoint Name - STRING [40]<br>Return Code - FOUR_BYTES<br>Function Name - STRING [64]<br>Calling Function - STRING [64]<br>Index - FOUR_BYTES                  |
| PRIMARY CAUSE    | A signaling adapter has detected an error while accessing a database interface.                                                                                 |
| PRIMARY ACTION   | If the database that the adapter attempted to access is not available, restart the associated process.                                                          |
| SECONDARY ACTION | If an incompatible versions of the signaling adapter process and the database processes are present on the system, correct the error and restart the processes. |

## SIGNALING (7)

To troubleshoot and correct the cause of the alarm, refer to the [“Socket Failure - Signaling \(7\)”](#) section on page 10-106.

|                 |                                                                                                                                  |
|-----------------|----------------------------------------------------------------------------------------------------------------------------------|
| DESCRIPTION     | Socket Failure                                                                                                                   |
| SEVERITY        | MAJOR                                                                                                                            |
| THRESHOLD       | 30                                                                                                                               |
| THROTTLE        | 0                                                                                                                                |
| DATAWORDS       | Reason Text - STRING [30]                                                                                                        |
| PRIMARY CAUSE   | Issued when there is a failure in creating the UDP port used by the MGCP stacks.                                                 |
| PRIMARY ACTION  | Reconfigure the MGCP stack to use a free UDP port.                                                                               |
| SECONDARY CAUSE | Some other application may already be active on the same UDP port and IP address to which the Call Agent MGCP stack is assigned. |

## SIGNALING (8)

To troubleshoot and correct the cause of the alarm, refer to the [“Session Initiation Protocol Message Receive Failure - Signaling \(8\)”](#) section on page 10-106.

|                |                                                                                                                                                                                            |
|----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| DESCRIPTION    | Session Initiation Protocol Message Receive Failure (SIP Message Receive Failure)                                                                                                          |
| SEVERITY       | MAJOR                                                                                                                                                                                      |
| THRESHOLD      | 30                                                                                                                                                                                         |
| THROTTLE       | 0                                                                                                                                                                                          |
| DATAWORDS      | Reason Text - STRING [50]                                                                                                                                                                  |
| PRIMARY CAUSE  | Operating system level network errors or invalid network configuration.                                                                                                                    |
| PRIMARY ACTION | Have your network administrator resolve network errors. Contact Cisco TAC if you need assistance. Manually clear alarm. Restart this call agent instance using the platform start command. |

Refer to the [“Obtaining Technical Assistance”](#) section on page xxxviii for detailed instructions on contacting Cisco TAC and opening a service request.

## SIGNALING (9)

To troubleshoot and correct the cause of the alarm, refer to the [“Timeout on Internet Protocol Address - Signaling \(9\)”](#) section on page 10-107.

|                  |                                                                                                                                                                                                                |
|------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| DESCRIPTION      | Timeout on Internet Protocol Address (Timeout on IP Address)                                                                                                                                                   |
| SEVERITY         | MAJOR                                                                                                                                                                                                          |
| THRESHOLD        | 100                                                                                                                                                                                                            |
| THROTTLE         | 0                                                                                                                                                                                                              |
| DATAWORDS        | MGW/Term Name - STRING [80]<br>Gateway Type - STRING [32]<br>Possible Cause - STRING [32]                                                                                                                      |
| PRIMARY CAUSE    | Issued when optcall is unable to communicate with a gateway.                                                                                                                                                   |
| PRIMARY ACTION   | Verify that the gateway is both configured for service and that it has been set in service.                                                                                                                    |
| SECONDARY ACTION | Attempt to ping the gateway using the Internet Protocol (IP) address from the event report. If the ping is not successful, then diagnose the issue that prevents the address from being reached.               |
| TERNARY ACTION   | Use the status media gateway (MGW) identification (ID) = xxx, where xxx is the IP address given in the event report. If the status is not in service (INS), then use control mgw command to put it in service. |



## SIGNALING (10)

To troubleshoot and correct the cause of the alarm, refer to the [“Failed to Send Complete Session Initiation Protocol Message - Signaling \(10\)”](#) section on page 10-107.

|                |                                                                                                                                                                     |
|----------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| DESCRIPTION    | Failed to Send Complete Session Initiation Protocol Message (Failed to Send Complete SIP Message)                                                                   |
| SEVERITY       | MINOR                                                                                                                                                               |
| THRESHOLD      | 100                                                                                                                                                                 |
| THROTTLE       | 0                                                                                                                                                                   |
| DATAWORDS      | Destination Address - STRING [64]                                                                                                                                   |
| PRIMARY CAUSE  | Notifies the user that the Session Initiation Protocol (SIP) stack failed to send an SIP message due to it exceeding the maximum length of a UDP packet.            |
| PRIMARY ACTION | If encountered in normal network operations, the message should be captured on passive testing equipment and sent to Cisco TAC for evaluation. (Contact Cisco TAC.) |

Refer to the [“Obtaining Technical Assistance”](#) section on page xxxviii for detailed instructions on contacting Cisco TAC and opening a service request.

## SIGNALING (11)

To troubleshoot and correct the cause of the alarm, refer to the [“Failed to Allocate Session Initiation Protocol Control Block - Signaling \(11\)”](#) section on page 10-107.

|                  |                                                                                                     |
|------------------|-----------------------------------------------------------------------------------------------------|
| DESCRIPTION      | Failed to Allocate Session Initiation Protocol Control Block (Failed to Allocate SIP Control Block) |
| SEVERITY         | MAJOR                                                                                               |
| THRESHOLD        | 100                                                                                                 |
| THROTTLE         | 0                                                                                                   |
| DATAWORDS        | Size - TWO_BYTES<br>Detail - STRING [80]                                                            |
| PRIMARY CAUSE    | Issued when there is not enough memory to allocate a SIP call control block.                        |
| PRIMARY ACTION   | Increase the SIP call control block (CCB) count specified in mem.cfg file.                          |
| SECONDARY ACTION | Restart call agent to take effect.                                                                  |

## SIGNALING (12)

To troubleshoot and correct the cause of the alarm, refer to the [“Feature Server is not Up or is not Responding to Call Agent - Signaling \(12\)”](#) section on page 10-108.

|                |                                                                    |
|----------------|--------------------------------------------------------------------|
| DESCRIPTION    | Feature Server is not Up or is not Responding to Call Agent        |
| SEVERITY       | CRITICAL                                                           |
| THRESHOLD      | 30                                                                 |
| THROTTLE       | 0                                                                  |
| DATAWORDS      | Domain Name of FS - STRING [65]<br>Feature Server ID - STRING [20] |
| PRIMARY CAUSE  | Feature server platform is down or is not operating properly.      |
| PRIMARY ACTION | Restart the applicable feature server.                             |

## SIGNALING (13)

To troubleshoot and correct the cause of the alarm, refer to the [“Signaling System 7 Signaling Link Down - Signaling \(13\)”](#) section on page 10-108.

|                   |                                                                      |
|-------------------|----------------------------------------------------------------------|
| DESCRIPTION       | Signaling System 7 Signaling Link Down (SS7 Signaling Link Down)     |
| SEVERITY          | MAJOR                                                                |
| THRESHOLD         | 100                                                                  |
| THROTTLE          | 0                                                                    |
| DATAWORDS         | Link_Number - ONE_BYTE<br>Link_Name - STRING [25]                    |
| PRIMARY CAUSE     | Signaling System 7 (SS7) trunk group may be out-of-service (OOS).    |
| PRIMARY ACTION    | Use control ss7-trunk-grp to place the trunk group in service (INS). |
| SECONDARY CAUSE   | The local Ulticom stack may be down.                                 |
| SECONDARY ACTION  | Run the Ulticom stack again.                                         |
| TERNARY CAUSE     | SS7 link may be disconnected or faulty.                              |
| TERNARY ACTION    | Check the Ulticom local configuration.                               |
| SUBSEQUENT CAUSE  | Remote SS7 signaling site may be down or incorrectly configured.     |
| SUBSEQUENT ACTION | Check the Ulticom remote configuration.                              |

## SIGNALING (14)

To troubleshoot and correct the cause of the alarm, refer to the [“Link is Remotely Inhibited - Signaling \(14\)” section on page 10-108](#).

|                |                                                                                                                                         |
|----------------|-----------------------------------------------------------------------------------------------------------------------------------------|
| DESCRIPTION    | Link is Remotely Inhibited                                                                                                              |
| SEVERITY       | MINOR                                                                                                                                   |
| THRESHOLD      | 100                                                                                                                                     |
| THROTTLE       | 0                                                                                                                                       |
| DATAWORDS      | Link - ONE_BYTE<br>Link Name - STRING [8]                                                                                               |
| PRIMARY CAUSE  | Issued when the specified Signaling System 7 (SS7) link is inhibited at the remote end.                                                 |
| PRIMARY ACTION | Monitor events at the network level for any related to the specified SS7 link. Restorative actions needs to be taken on the remote end. |

## SIGNALING (15)

To troubleshoot and correct the cause of the alarm, refer to the [“Link is Locally Inhibited - Signaling \(15\)” section on page 10-108](#).

|                  |                                                                                                             |
|------------------|-------------------------------------------------------------------------------------------------------------|
| DESCRIPTION      | Link is Locally Inhibited                                                                                   |
| SEVERITY         | MINOR                                                                                                       |
| THRESHOLD        | 100                                                                                                         |
| THROTTLE         | 0                                                                                                           |
| DATAWORDS        | Link No - ONE_BYTE<br>Link Name - STRING [8]                                                                |
| PRIMARY CAUSE    | Issued when the specified SS7 link is inhibited at the local end.                                           |
| PRIMARY ACTION   | Verify that the SS7 signaling adapter process is running and that the SS7 interface card(s) are in service. |
| SECONDARY ACTION | If a component is found to be non-operational, restore it to service.                                       |

## SIGNALING (16)

To troubleshoot and correct the cause of the alarm, refer to the [“Link is Congested - Signaling \(16\)” section on page 10-109](#).

|                   |                                                                                                                                                                                                |
|-------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| DESCRIPTION       | Link is Congested                                                                                                                                                                              |
| SEVERITY          | MINOR                                                                                                                                                                                          |
| THRESHOLD         | 100                                                                                                                                                                                            |
| THROTTLE          | 0                                                                                                                                                                                              |
| DATAWORDS         | Link No - ONE_BYTE                                                                                                                                                                             |
| PRIMARY CAUSE     | Issued when the specified SS7 link is experiencing congestion.                                                                                                                                 |
| PRIMARY ACTION    | Monitor event reports at the network level to determine if the traffic load on the specified SS7 link is too high on the local end, or if the remote end is lagging in processing the traffic. |
| SECONDARY ACTION  | Verify that the SS7 link has not degraded in quality.                                                                                                                                          |
| TERNARY ACTION    | Verify that the traffic load has not become unbalanced if multiple SS7 links are used.                                                                                                         |
| SUBSEQUENT ACTION | Verify that local SS7 signaling adapter process is running normally.                                                                                                                           |

## SIGNALING (17)

To troubleshoot and correct the cause of the alarm, refer to the [“Link: Local Processor Outage - Signaling \(17\)” section on page 10-109](#).

|                |                                                                                                                                                                                                                                            |
|----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| DESCRIPTION    | Link: Local Processor Outage                                                                                                                                                                                                               |
| SEVERITY       | MINOR                                                                                                                                                                                                                                      |
| THRESHOLD      | 100                                                                                                                                                                                                                                        |
| THROTTLE       | 0                                                                                                                                                                                                                                          |
| DATAWORDS      | Link No - ONE_BYTE<br>Link Name - STRING [8]                                                                                                                                                                                               |
| PRIMARY CAUSE  | Issued when the specified SS7 link has experienced a processor outage.                                                                                                                                                                     |
| PRIMARY ACTION | Monitor the system for maintenance event reports associated with the signaling adapter or underlying platform instance that support the specified SS7 link. Verify that the process and or platform are restarted and returned to service. |

## SIGNALING (18)

To troubleshoot and correct the cause of the alarm, refer to the [“Link: Remote Processor Outage - Signaling \(18\)” section on page 10-109](#).

|                |                                                                                                                                                                                |
|----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| DESCRIPTION    | Link: Remote Processor Outage                                                                                                                                                  |
| SEVERITY       | MINOR                                                                                                                                                                          |
| THRESHOLD      | 100                                                                                                                                                                            |
| THROTTLE       | 0                                                                                                                                                                              |
| DATAWORDS      | Link No - ONE_BYTE<br>Link Name - STRING [8]                                                                                                                                   |
| PRIMARY CAUSE  | Issued when the specified SS7 link has experienced a processor outage.                                                                                                         |
| PRIMARY ACTION | Monitor the network level event reports for any events associated with the processing complex used by the specified SS7 link. Verify that the SS7 link is returned to service. |

## SIGNALING (19)

To troubleshoot and correct the cause of the alarm, refer to the [“Link Set Inaccessible - Signaling \(19\)” section on page 10-109](#).

|                |                                                                                                                                    |
|----------------|------------------------------------------------------------------------------------------------------------------------------------|
| DESCRIPTION    | Link Set Inaccessible                                                                                                              |
| SEVERITY       | MAJOR                                                                                                                              |
| THRESHOLD      | 100                                                                                                                                |
| THROTTLE       | 0                                                                                                                                  |
| DATAWORDS      | Link Set No - ONE_BYTE<br>Link Set Name - STRING [8]                                                                               |
| PRIMARY CAUSE  | Issued when the specified SS7 link set is inaccessible.                                                                            |
| PRIMARY ACTION | If the SS7 signaling adapter is not running normally and the associated call agent platform is not active, return them to service. |

## SIGNALING (20)

To troubleshoot and correct the cause of the alarm, refer to the [“Link Set Congestion - Signaling \(20\)” section on page 10-109](#).

|                   |                                                                                                                                                                                                    |
|-------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| DESCRIPTION       | Link Set Congestion                                                                                                                                                                                |
| SEVERITY          | MAJOR                                                                                                                                                                                              |
| THRESHOLD         | 100                                                                                                                                                                                                |
| THROTTLE          | 0                                                                                                                                                                                                  |
| DATAWORDS         | Link Set No - ONE_BYTE<br>Link Set Name - STRING [8]<br>Congestion Level - ONE_BYTE                                                                                                                |
| PRIMARY CAUSE     | Issued when the specified SS7 link set is experiencing congestion.                                                                                                                                 |
| PRIMARY ACTION    | Monitor event reports at the network level to determine if the traffic load on the specified SS7 link set is too high on the local end, or if the remote end is lagging in processing the traffic. |
| SECONDARY ACTION  | Verify that the SS7 link set has not degraded in quality.                                                                                                                                          |
| TERNARY ACTION    | Verify that the traffic load has not become unbalanced if multiple SS7 link sets are used.                                                                                                         |
| SUBSEQUENT ACTION | Verify that local SS7 signaling adapter process is running normally.                                                                                                                               |

## SIGNALING (21)

To troubleshoot and correct the cause of the alarm, refer to the [“Route Set Failure - Signaling \(21\)” section on page 10-110](#).

|                  |                                                                                                                   |
|------------------|-------------------------------------------------------------------------------------------------------------------|
| DESCRIPTION      | Route Set Failure                                                                                                 |
| SEVERITY         | MAJOR                                                                                                             |
| THRESHOLD        | 200                                                                                                               |
| THROTTLE         | 0                                                                                                                 |
| DATAWORDS        | Route Set No - TWO_BYTES<br>Route Set Name - STRING [8]                                                           |
| PRIMARY CAUSE    | Issued when the specified route set has experienced a failure.                                                    |
| PRIMARY ACTION   | Verify that the processing complex supporting the route set is functional.                                        |
| SECONDARY ACTION | Monitor event reports at the network level to determine the failing component and verify its restoral to service. |

## SIGNALING (22)

To troubleshoot and correct the cause of the alarm, refer to the [“Route Set Congested - Signaling \(22\)” section on page 10-110](#).

|                   |                                                                                                                                                                                                    |
|-------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| DESCRIPTION       | Route Set Congested                                                                                                                                                                                |
| SEVERITY          | MINOR                                                                                                                                                                                              |
| THRESHOLD         | 100                                                                                                                                                                                                |
| THROTTLE          | 0                                                                                                                                                                                                  |
| DATAWORDS         | Route Set No - TWO_BYTES<br>Route Set Name - STRING [8]<br>Congestion Level - ONE_BYTE                                                                                                             |
| PRIMARY CAUSE     | Issued when the specified route set is experiencing congestion.                                                                                                                                    |
| PRIMARY ACTION    | Monitor event reports at the network level to determine if the traffic load on the specified SS7 link set is too high on the local end, or if the remote end is lagging in processing the traffic. |
| SECONDARY ACTION  | Verify that the SS7 link set has not degraded in quality.                                                                                                                                          |
| TERNARY ACTION    | Verify that the traffic load has not become unbalanced if multiple SS7 link sets are used.                                                                                                         |
| SUBSEQUENT ACTION | Verify that local SS7 signaling adapter process is running normally.                                                                                                                               |

## SIGNALING (23)

To troubleshoot and correct the cause of the alarm, refer to the [“Destination Point Code Unavailable - Signaling \(23\)” section on page 10-111](#).

|                |                                                                                                                                                                                                                                                       |
|----------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| DESCRIPTION    | Destination Point Code Unavailable (DPC Unavailable)                                                                                                                                                                                                  |
| SEVERITY       | MAJOR                                                                                                                                                                                                                                                 |
| THRESHOLD      | 200                                                                                                                                                                                                                                                   |
| THROTTLE       | 0                                                                                                                                                                                                                                                     |
| DATAWORDS      | DPC - STRING [12]                                                                                                                                                                                                                                     |
| PRIMARY CAUSE  | Issued when the specified destination point code (DPC) is not available. This is usually caused by one of the following:<br>1) A failure in the affected DPC.<br>2) An unavailable route between the Cisco BTS 10200 Softswitch and the affected DPC. |
| PRIMARY ACTION | Verify that alternate routing has been assigned for traffic destined to the affected DPC.                                                                                                                                                             |

## SIGNALING (24)

To troubleshoot and correct the cause of the alarm, refer to the [“Destination Point Code Congested - Signaling \(24\)” section on page 10-112](#).

|                |                                                                                                                                                                                           |
|----------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| DESCRIPTION    | Destination Point Code Congested (DPC Congested)                                                                                                                                          |
| SEVERITY       | MINOR                                                                                                                                                                                     |
| THRESHOLD      | 100                                                                                                                                                                                       |
| THROTTLE       | 0                                                                                                                                                                                         |
| DATAWORDS      | DPC - STRING [12]<br>DPC Type - ONE_BYTE<br>Congestion Level - ONE_BYTE                                                                                                                   |
| PRIMARY CAUSE  | Issued when the specified destination point code is congested.                                                                                                                            |
| PRIMARY ACTION | Monitor event reports at the network level to determine if the traffic load to the specified DPC is too high on the local end, or if the remote end is lagging in processing the traffic. |

## SIGNALING (25)

To monitor and correct the cause of the event, refer to the [“Unanswered Blocking Message - Signaling \(25\)” section on page 10-83](#).

|                   |                                                                                                                                                    |
|-------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|
| DESCRIPTION       | Unanswered Blocking Message (Unanswered BLO)                                                                                                       |
| SEVERITY          | WARNING                                                                                                                                            |
| THRESHOLD         | 100                                                                                                                                                |
| THROTTLE          | 0                                                                                                                                                  |
| DATAWORDS         | CIC Number - TWO_BYTES<br>TGN-ID - FOUR_BYTES<br>DPC - STRING [20]<br>OPC - STRING [20]                                                            |
| PRIMARY CAUSE     | Issued when a blocking (BLO) message was not acknowledged before the timer T13 (T13) expired for the associated circuit identification code (CIC). |
| PRIMARY ACTION    | Verify that the SS7 signaling adapter processes is running normally. Verify that the call agent platform is active.                                |
| SECONDARY ACTION  | Verify that the SS7 interface hardware is in service. Verify that the associated SS7 signaling link is available.                                  |
| TERNARY ACTION    | Verify that the T13 timer is set to an appropriate level.                                                                                          |
| SUBSEQUENT ACTION | Verify that the SS7 link is not congested.                                                                                                         |



## SIGNALING (26)

To monitor and correct the cause of the event, refer to the [“Unanswered Unblocking Message - Signaling \(26\)” section on page 10-83](#).

|                   |                                                                                                                               |
|-------------------|-------------------------------------------------------------------------------------------------------------------------------|
| DESCRIPTION       | Unanswered Unblocking Message (Unanswered UBL)                                                                                |
| SEVERITY          | WARNING                                                                                                                       |
| THRESHOLD         | 100                                                                                                                           |
| THROTTLE          | 0                                                                                                                             |
| DATAWORDS         | CIC Number - TWO_BYTES<br>TGN-ID - FOUR_BYTES<br>DPC - STRING [20]<br>OPC - STRING [20]                                       |
| PRIMARY CAUSE     | Issued when a unblocking message (UBL) message was not acknowledged before the timer 15 (T15) expired for the associated CIC. |
| PRIMARY ACTION    | Verify that the SS7 signaling adapter processes is running normally. Verify that the call agent platform is active.           |
| SECONDARY ACTION  | Verify that the SS7 interface hardware is in service. Verify that the associated SS7 signaling link is available.             |
| TERNARY ACTION    | Verify that the T13 timer is set to an appropriate level.                                                                     |
| SUBSEQUENT ACTION | Verify that the SS7 link is not congested.                                                                                    |

## SIGNALING (27)

To monitor and correct the cause of the event, refer to the [“Unanswered Circuit Group Blocking Message - Signaling \(27\)” section on page 10-83](#).

|                   |                                                                                                                                   |
|-------------------|-----------------------------------------------------------------------------------------------------------------------------------|
| DESCRIPTION       | Unanswered Circuit Group Blocking Message (Unanswered CGB)                                                                        |
| SEVERITY          | WARNING                                                                                                                           |
| THRESHOLD         | 100                                                                                                                               |
| THROTTLE          | 0                                                                                                                                 |
| DATAWORDS         | CIC Number - TWO_BYTES<br>TGN-ID - FOUR_BYTES<br>DPC - STRING [20]<br>OPC - STRING [20]                                           |
| PRIMARY CAUSE     | Issued when a circuit group blocking (CGB) message was not acknowledged before the timer 19 (T19) expired for the associated CIC. |
| PRIMARY ACTION    | Verify that the SS7 signaling adapter processes is running normally. Verify that the call agent platform is active.               |
| SECONDARY ACTION  | Verify that the SS7 interface hardware is in service. Verify that the associated SS7 signaling link is available.                 |
| TERNARY ACTION    | Verify that the T13 timer is set to an appropriate level.                                                                         |
| SUBSEQUENT ACTION | Verify that the SS7 link is not congested.                                                                                        |

## SIGNALING (28)

To monitor and correct the cause of the event, refer to the [“Unanswered Circuit Group Unblocking Message - Signaling \(28\)”](#) section on page 10-84.

|                   |                                                                                                                                                                  |
|-------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| DESCRIPTION       | Unanswered Circuit Group Unblocking Message (Unanswered CGU)                                                                                                     |
| SEVERITY          | WARNING                                                                                                                                                          |
| THRESHOLD         | 100                                                                                                                                                              |
| THROTTLE          | 0                                                                                                                                                                |
| DATAWORDS         | CIC Number - TWO_BYTES<br>TGN-ID - FOUR_BYTES<br>DPC - STRING [20]<br>OPC - STRING [20]                                                                          |
| PRIMARY CAUSE     | Issued when a circuit group unblocking (CGU) message was not acknowledged before the timer 21 (T21) expired for the associated CIC.                              |
| PRIMARY ACTION    | Verify that the SS7 signaling adapter processes is running normally.                                                                                             |
| SECONDARY ACTION  | Verify that the call agent platform is active.                                                                                                                   |
| TERNARY ACTION    | Verify that the SS7 interface hardware is in service.                                                                                                            |
| SUBSEQUENT ACTION | Verify that the associated SS7 signaling link is available. Verify that the T13 timer is set to an appropriate level. Verify that the SS7 link is not congested. |

## SIGNALING (29)

To monitor and correct the cause of the event, refer to the [“Unanswered Circuit Query Message - Signaling \(29\)”](#) section on page 10-84.

|                   |                                                                                                                                  |
|-------------------|----------------------------------------------------------------------------------------------------------------------------------|
| DESCRIPTION       | Unanswered Circuit Query Message (Unanswered CQM)                                                                                |
| SEVERITY          | WARNING                                                                                                                          |
| THRESHOLD         | 100                                                                                                                              |
| THROTTLE          | 0                                                                                                                                |
| DATAWORDS         | CIC Number - TWO_BYTES<br>TGN-ID - FOUR_BYTES<br>DPC - STRING [20]<br>OPC - STRING [20]                                          |
| PRIMARY CAUSE     | Issued when a circuit query message (CQM) message was not acknowledged before the timer 28 (T28) expired for the associated CIC. |
| PRIMARY ACTION    | Verify that the SS7 signaling adapter processes is running normally.                                                             |
| SECONDARY ACTION  | Verify that the call agent platform is active. Verify that the SS7 interface hardware is in service.                             |
| TERNARY ACTION    | Verify that the associated SS7 signaling link is available.                                                                      |
| SUBSEQUENT ACTION | Verify that the T13 timer is set to an appropriate level. Verify that the SS7 link is not congested.                             |

## SIGNALING (30)

To monitor and correct the cause of the event, refer to the [“Unanswered Circuit Validation Test Message - Signaling \(30\)” section on page 10-84](#).

|                   |                                                                                                                                                                  |
|-------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| DESCRIPTION       | Unanswered Circuit Validation Test Message (Unanswered CVT)                                                                                                      |
| SEVERITY          | WARNING                                                                                                                                                          |
| THRESHOLD         | 100                                                                                                                                                              |
| THROTTLE          | 0                                                                                                                                                                |
| DATAWORDS         | CIC Number - TWO_BYTES<br>TGN-ID - FOUR_BYTES<br>DPC - STRING [20]<br>OPC - STRING [20]                                                                          |
| PRIMARY CAUSE     | Issued when a circuit validation test (CVT) message was not acknowledged before the Tcvt expired for the associated CIC.                                         |
| PRIMARY ACTION    | Verify that the SS7 signaling adapter processes is running normally.                                                                                             |
| SECONDARY ACTION  | Verify that the call agent platform is active.                                                                                                                   |
| TERNARY ACTION    | Verify that the SS7 interface hardware is in service.                                                                                                            |
| SUBSEQUENT ACTION | Verify that the associated SS7 signaling link is available. Verify that the T13 timer is set to an appropriate level. Verify that the SS7 link is not congested. |

## SIGNALING (31)

To monitor and correct the cause of the event, refer to the [“Unanswered Reset Circuit Message - Signaling \(31\)”](#) section on page 10-84.

|                   |                                                                                                                          |
|-------------------|--------------------------------------------------------------------------------------------------------------------------|
| DESCRIPTION       | Unanswered Reset Circuit Message (Unanswered RSC)                                                                        |
| SEVERITY          | WARNING                                                                                                                  |
| THRESHOLD         | 100                                                                                                                      |
| THROTTLE          | 0                                                                                                                        |
| DATAWORDS         | CIC Number - TWO_BYTES<br>TGN-ID - FOUR_BYTES<br>DPC - STRING [20]<br>OPC - STRING [20]                                  |
| PRIMARY CAUSE     | Issued when a reset circuit (RSC) message was not acknowledged before the timer 17 (T17) expired for the associated CIC. |
| PRIMARY ACTION    | Verify that the SS7 signaling adapter processes is running normally. Verify that the call agent platform is active.      |
| SECONDARY ACTION  | Verify that the SS7 interface hardware is in service. Verify that the associated SS7 signaling link is available.        |
| TERNARY ACTION    | Verify that the T13 timer is set to an appropriate level.                                                                |
| SUBSEQUENT ACTION | Verify that the SS7 link is not congested.                                                                               |

## SIGNALING (32)

To monitor and correct the cause of the event, refer to the [“Unanswered Group Reset Message - Signaling \(32\)” section on page 10-84](#).

|                   |                                                                                                                        |
|-------------------|------------------------------------------------------------------------------------------------------------------------|
| DESCRIPTION       | Unanswered Group Reset Message (Unanswered GRS)                                                                        |
| SEVERITY          | WARNING                                                                                                                |
| THRESHOLD         | 100                                                                                                                    |
| THROTTLE          | 0                                                                                                                      |
| DATAWORDS         | CIC Number - TWO_BYTES<br>TGN-ID - FOUR_BYTES<br>DPC - STRING [20]<br>OPC - STRING [20]                                |
| PRIMARY CAUSE     | Issued when a group reset (GRS) message was not acknowledged before the timer 23 (T23) expired for the associated CIC. |
| PRIMARY ACTION    | Verify that the SS7 signaling adapter processes is running normally. Verify that the call agent platform is active.    |
| SECONDARY ACTION  | Verify that the SS7 interface hardware is in service. Verify that the associated SS7 signaling link is available.      |
| TERNARY ACTION    | Verify that the T13 timer is set to an appropriate level.                                                              |
| SUBSEQUENT ACTION | Verify that the SS7 link is not congested.                                                                             |

## SIGNALING (33)

To monitor and correct the cause of the event, refer to the [“Unanswered Release Message - Signaling \(33\)” section on page 10-85](#).

|                   |                                                                                                                       |
|-------------------|-----------------------------------------------------------------------------------------------------------------------|
| DESCRIPTION       | Unanswered Release Message (Unanswered REL)                                                                           |
| SEVERITY          | WARNING                                                                                                               |
| THRESHOLD         | 100                                                                                                                   |
| THROTTLE          | 0                                                                                                                     |
| DATAWORDS         | CIC Number - TWO_BYTES<br>TGN-ID - FOUR_BYTES<br>DPC - STRING [20]<br>OPC - STRING [20]                               |
| PRIMARY CAUSE     | Issued when a release (REL) message was not acknowledged before the timer 5 (T5) expired for the associated CIC.      |
| PRIMARY ACTION    | Verify that the SS7 signaling adapter processes is running normally.                                                  |
| SECONDARY ACTION  | Verify that the call agent platform is active. Verify that the SS7 interface hardware is in service.                  |
| TERNARY ACTION    | Verify that the associated SS7 signaling link is available. Verify that the T13 timer is set to an appropriate level. |
| SUBSEQUENT ACTION | Verify that the SS7 link is not congested.                                                                            |



## SIGNALING (34)

To monitor and correct the cause of the event, refer to the [“Unanswered Continuity Check Request Message - Signaling \(34\)”](#) section on page 10-85.

|                   |                                                                                                                                                                                 |
|-------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| DESCRIPTION       | Unanswered Continuity Check Request Message (Unanswered CCR)                                                                                                                    |
| SEVERITY          | WARNING                                                                                                                                                                         |
| THRESHOLD         | 100                                                                                                                                                                             |
| THROTTLE          | 0                                                                                                                                                                               |
| DATAWORDS         | CIC Number - TWO_BYTES<br>TGN-ID - FOUR_BYTES<br>DPC - STRING [20]<br>OPC - STRING [20]                                                                                         |
| PRIMARY CAUSE     | Issued when an loop prevention acknowledgement (LPA) message was not acknowledged before the timer continuity check request (T <sub>CCR</sub> ) expired for the associated CIC. |
| PRIMARY ACTION    | Verify that the SS7 signaling adapter processes is running normally.                                                                                                            |
| SECONDARY ACTION  | Verify that the call agent platform is active.                                                                                                                                  |
| TERNARY ACTION    | Verify that the SS7 interface hardware is in service.                                                                                                                           |
| SUBSEQUENT ACTION | Verify that the associated SS7 signaling link is available. Verify that the T13 timer is set to an appropriate level. Verify that the SS7 link is not congested.                |



### Note

SIGNALING (35) is not used.

## SIGNALING (36)

To troubleshoot and correct the cause of the alarm, refer to the [“Trunk Locally Blocked - Signaling \(36\)” section on page 10-112](#). For additional troubleshooting information, refer to [Appendix A, “System Usage of MGW Keepalive Parameters, Release 4.4.x.”](#)

|                |                                                                                                                                                                               |
|----------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| DESCRIPTION    | Trunk Locally Blocked                                                                                                                                                         |
| SEVERITY       | MINOR                                                                                                                                                                         |
| THRESHOLD      | 500                                                                                                                                                                           |
| THROTTLE       | 0                                                                                                                                                                             |
| DATAWORDS      | CIC Number - STRING [40]<br>TGN-ID - FOUR_BYTES<br>DPC - STRING [20]<br>OPC - STRING [20]<br>MGW-EP-NAME - STRING [64]<br>MGW-TSAP-ADDR - STRING [80]<br>Reason - STRING [80] |
| PRIMARY CAUSE  | Issued when a BLO or CGB message was sent on the specified CIC.                                                                                                               |
| PRIMARY ACTION | Refer to <a href="#">Appendix A, “System Usage of MGW Keepalive Parameters, Release 4.4.x.”</a>                                                                               |

**Note**

SIGNALING (37) through SIGNALING (39) are not used.

## SIGNALING (40)

To troubleshoot and correct the cause of the alarm, refer to the [“Trunk Remotely Blocked - Signaling \(40\)” section on page 10-112.](#)

|                |                                                                                                                                                                                                                                                                                                           |
|----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| DESCRIPTION    | Trunk Remotely Blocked                                                                                                                                                                                                                                                                                    |
| SEVERITY       | MAJOR                                                                                                                                                                                                                                                                                                     |
| THRESHOLD      | 500                                                                                                                                                                                                                                                                                                       |
| THROTTLE       | 0                                                                                                                                                                                                                                                                                                         |
| DATAWORDS      | CIC Number - STRING [40]<br>TGN-ID - FOUR_BYTES<br>DPC - STRING [20]<br>OPC - STRING [20]<br>MGW-EP-NAME - STRING [64]<br>MGW-TSAP-ADDR - STRING [80]                                                                                                                                                     |
| PRIMARY CAUSE  | Issued when a BLO or CGB message was received on the specified CIC if it is SS7 trunk. Issued when a SERVICE OOS message is received for Integrated Services Digital Network (ISDN) trunks. Issued when Reverse Make Busy (RBZ) signal is received for channel-associated signaling (CAS) operator trunk. |
| PRIMARY ACTION | No action required. Can manually recover from this condition locally by controlling effected trunks to unequipped (UEQP) state and back INS.                                                                                                                                                              |



### Note

SIGNALING (41) is not used.

## SIGNALING (42)

For additional information, refer to the [“Continuity Testing Message Received on the Specified Circuit Identification Code - Signaling \(42\)” section on page 10-85.](#)

|                |                                                                                                                              |
|----------------|------------------------------------------------------------------------------------------------------------------------------|
| DESCRIPTION    | Continuity Testing Message Received on the Specified Circuit Identification Code (COT Message Received on the Specified CIC) |
| SEVERITY       | INFO                                                                                                                         |
| THRESHOLD      | 100                                                                                                                          |
| THROTTLE       | 0                                                                                                                            |
| DATAWORDS      | CIC Number - TWO_BYTES<br>TGN-ID - FOUR_BYTES<br>DPC - STRING [20]<br>OPC - STRING [20]                                      |
| PRIMARY CAUSE  | Issued when a continuity testing (COT) message was received on the specified CIC.                                            |
| PRIMARY ACTION | No action required.                                                                                                          |

## SIGNALING (43)

For additional information, refer to the [“Release Complete Received in Response to Reset Circuit Message on the Specified Circuit Identification Code - Signaling \(43\)”](#) section on page 10-86.

|                |                                                                                                                                                                            |
|----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| DESCRIPTION    | Release Complete Received in Response to Reset Circuit Message on the Specified Circuit Identification Code (RLC Received in Response to RSC Message on the Specified CIC) |
| SEVERITY       | INFO                                                                                                                                                                       |
| THRESHOLD      | 100                                                                                                                                                                        |
| THROTTLE       | 0                                                                                                                                                                          |
| DATAWORDS      | CIC Number - TWO_BYTES<br>TGN-ID - FOUR_BYTES<br>DPC - STRING [20]<br>OPC - STRING [20]                                                                                    |
| PRIMARY CAUSE  | Issued when a release complete (RLC) message was received in response to a RSC message on the specified CIC.                                                               |
| PRIMARY ACTION | No action required.                                                                                                                                                        |

## SIGNALING (44)

For additional information, refer to the [“Continuity Recheck is Performed on Specified Circuit Identification Code - Signaling \(44\)”](#) section on page 10-86.

|                |                                                                                                                             |
|----------------|-----------------------------------------------------------------------------------------------------------------------------|
| DESCRIPTION    | Continuity Recheck is Performed on Specified Circuit Identification Code (Continuity Recheck is Performed on Specified CIC) |
| SEVERITY       | INFO                                                                                                                        |
| THRESHOLD      | 100                                                                                                                         |
| THROTTLE       | 0                                                                                                                           |
| DATAWORDS      | CIC Number - TWO_BYTES<br>TGN-ID - FOUR_BYTES<br>DPC - STRING [20]<br>OPC - STRING [20]                                     |
| PRIMARY CAUSE  | Issued when a continuity recheck was performed on the specified CIC.                                                        |
| PRIMARY ACTION | No action required.                                                                                                         |

## SIGNALING (45)

For additional information, refer to the [“Circuit is UNEQUIPPED on Remote Side - Signaling \(45\)” section on page 10-86](#).

|                |                                                                                                                                              |
|----------------|----------------------------------------------------------------------------------------------------------------------------------------------|
| DESCRIPTION    | Circuit is UNEQUIPPED on Remote Side                                                                                                         |
| SEVERITY       | INFO                                                                                                                                         |
| THRESHOLD      | 100                                                                                                                                          |
| THROTTLE       | 0                                                                                                                                            |
| DATAWORDS      | CIC Number - TWO_BYTES<br>TGN-ID - FOUR_BYTES<br>DPC - STRING [20]<br>OPC - STRING [20]                                                      |
| PRIMARY CAUSE  | Issued when an unequipped circuit has been detected on the remote side.                                                                      |
| PRIMARY ACTION | Monitor the event reports at the network level to verify if an existing circuit was unequipped causing a status mismatch with the local end. |

## SIGNALING (46)

For additional information, refer to the [“Specified Circuit Identification Code is Invalid for the Operation - Signaling \(46\)” section on page 10-86](#).

|                |                                                                                                                 |
|----------------|-----------------------------------------------------------------------------------------------------------------|
| DESCRIPTION    | Specified Circuit Identification Code is Invalid for the Operation (Specified CIC is Invalid for the Operation) |
| SEVERITY       | INFO                                                                                                            |
| THRESHOLD      | 100                                                                                                             |
| THROTTLE       | 0                                                                                                               |
| DATAWORDS      | CIC Number - TWO_BYTES<br>TGN-ID - FOUR_BYTES<br>DPC - STRING [20]<br>OPC - STRING [20]                         |
| PRIMARY CAUSE  | Issued when an invalid operation was performed on the specified CIC.                                            |
| PRIMARY ACTION | Verify that the SS7 provisioning tables are properly configured at the circuit level.                           |



### Note

SIGNALING (47) and SIGNALING (48) are not used.

## SIGNALING (49)

For additional information, refer to the [“A General Processing Error Encountered - Signaling \(49\)” section on page 10-86](#).

|                |                                                                                                                    |
|----------------|--------------------------------------------------------------------------------------------------------------------|
| DESCRIPTION    | A General Processing Error Encountered                                                                             |
| SEVERITY       | INFO                                                                                                               |
| THRESHOLD      | 100                                                                                                                |
| THROTTLE       | 0                                                                                                                  |
| DATAWORDS      | CIC Number - TWO_BYTES<br>TGN-ID - FOUR_BYTES<br>DPC - STRING [20]<br>OPC - STRING [20]                            |
| PRIMARY CAUSE  | Issued when a general SS7 processing error occurred due to all resources being busy or an invalid event occurring. |
| PRIMARY ACTION | Verify the status of the signaling adapter process and the SS7 signaling interface to verify proper operation.     |

## SIGNALING (50)

For additional information, refer to the [“Unexpected Message for the Call State is Received: Clear Call - Signaling \(50\)” section on page 10-86](#).

|                |                                                                                                                                     |
|----------------|-------------------------------------------------------------------------------------------------------------------------------------|
| DESCRIPTION    | Unexpected Message for the Call State is Received: Clear Call                                                                       |
| SEVERITY       | INFO                                                                                                                                |
| THRESHOLD      | 100                                                                                                                                 |
| THROTTLE       | 0                                                                                                                                   |
| DATAWORDS      | CIC Number - TWO_BYTES<br>TGN-ID - FOUR_BYTES<br>DPC - STRING [20]<br>OPC - STRING [20]                                             |
| PRIMARY CAUSE  | Issued when an unexpected message was received for the current call state.                                                          |
| PRIMARY ACTION | The call is cleared. Verify the status of the signaling adapter process and the SS7 signaling interface to verify proper operation. |

## SIGNALING (51)

For additional information, refer to the [“Set Trunk State as Remotely Unequipped - Signaling \(51\)” section on page 10-87](#).

|                |                                                                                                                                         |
|----------------|-----------------------------------------------------------------------------------------------------------------------------------------|
| DESCRIPTION    | Set Trunk State as Remotely Unequipped                                                                                                  |
| SEVERITY       | INFO                                                                                                                                    |
| THRESHOLD      | 100                                                                                                                                     |
| THROTTLE       | 0                                                                                                                                       |
| DATAWORDS      | CIC Number - TWO_BYTES<br>TGN-ID - FOUR_BYTES<br>DPC - STRING [20]<br>OPC - STRING [20]                                                 |
| PRIMARY CAUSE  | Issued when the specified CIC is marked at remotely unequipped due to the CQM response indicating that it is unequipped at the far end. |
| PRIMARY ACTION | Equip the trunk circuit at the far end.                                                                                                 |

## SIGNALING (52)

For additional information, refer to the [“Set Trunk State as NOT Remotely Blocked - Signaling \(52\)” section on page 10-87](#).

|                |                                                                                                                                                    |
|----------------|----------------------------------------------------------------------------------------------------------------------------------------------------|
| DESCRIPTION    | Set Trunk State as NOT Remotely Blocked                                                                                                            |
| SEVERITY       | INFO                                                                                                                                               |
| THRESHOLD      | 100                                                                                                                                                |
| THROTTLE       | 0                                                                                                                                                  |
| DATAWORDS      | CIC Number - TWO_BYTES<br>TGN-ID - FOUR_BYTES<br>DPC - STRING [20]<br>OPC - STRING [20]                                                            |
| PRIMARY CAUSE  | Issued when the specified CIC is marked as not remotely blocked due to the CQM response indicating that it is not remotely blocked at the far end. |
| PRIMARY ACTION | No action required.                                                                                                                                |

## SIGNALING (53)

For additional information, refer to the [“Set Trunk State as Remotely Blocked - Signaling \(53\)”](#) section on page 10-87.

|                |                                                                                                                                            |
|----------------|--------------------------------------------------------------------------------------------------------------------------------------------|
| DESCRIPTION    | Set Trunk State as Remotely Blocked                                                                                                        |
| SEVERITY       | INFO                                                                                                                                       |
| THRESHOLD      | 100                                                                                                                                        |
| THROTTLE       | 0                                                                                                                                          |
| DATAWORDS      | CIC Number - TWO_BYTES<br>TGN-ID - FOUR_BYTES<br>DPC - STRING [20]<br>OPC - STRING [20]                                                    |
| PRIMARY CAUSE  | Issued when the specified CIC is marked as remotely blocked due to the CQM response indicating that it is remotely blocked at the far end. |
| PRIMARY ACTION | Clear the blocking situation at the far end based on network level event reports.                                                          |

## SIGNALING (54)

For additional information, refer to the [“Circuit Validation Test Aborted - Signaling \(54\)”](#) section on page 10-87.

|                |                                                                                         |
|----------------|-----------------------------------------------------------------------------------------|
| DESCRIPTION    | Circuit Validation Test Aborted                                                         |
| SEVERITY       | INFO                                                                                    |
| THRESHOLD      | 100                                                                                     |
| THROTTLE       | 0                                                                                       |
| DATAWORDS      | CIC Number - TWO_BYTES<br>TGN-ID - FOUR_BYTES<br>DPC - STRING [20]<br>OPC - STRING [20] |
| PRIMARY CAUSE  | Issued when the circuit specified failed a validation test due to an internal failure.  |
| PRIMARY ACTION | Verify the SS7 signaling adapter process and SS7 interface is operating normally.       |



## SIGNALING (55)

For additional information, refer to the [“Circuit Validation Successful - Signaling \(55\)”](#) section on page 10-87.

|                |                                                                                         |
|----------------|-----------------------------------------------------------------------------------------|
| DESCRIPTION    | Circuit Validation Successful                                                           |
| SEVERITY       | INFO                                                                                    |
| THRESHOLD      | 100                                                                                     |
| THROTTLE       | 0                                                                                       |
| DATAWORDS      | CIC Number - TWO_BYTES<br>TGN-ID - FOUR_BYTES<br>DPC - STRING [20]<br>OPC - STRING [20] |
| PRIMARY CAUSE  | Issued when the specified circuit was successfully validated.                           |
| PRIMARY ACTION | No action required.                                                                     |



### Note

SIGNALING (56) is not used.

## SIGNALING (57)

For additional information, refer to the [“Continuity Recheck Failed - Signaling \(57\)”](#) section on page 10-87.

|                |                                                                                         |
|----------------|-----------------------------------------------------------------------------------------|
| DESCRIPTION    | Continuity Recheck Failed                                                               |
| SEVERITY       | INFO                                                                                    |
| THRESHOLD      | 100                                                                                     |
| THROTTLE       | 0                                                                                       |
| DATAWORDS      | CIC Number - TWO_BYTES<br>TGN-ID - FOUR_BYTES<br>DPC - STRING [20]<br>OPC - STRING [20] |
| PRIMARY CAUSE  | Issued when a continuity recheck of the specified CIC failed.                           |
| PRIMARY ACTION | Verify the SS7 signaling adapter process and SS7 interface is operating normally.       |

## SIGNALING (58)

For additional information, refer to the [“Continuity Recheck Successful - Signaling \(58\)”](#) section on page 10-87.

|                |                                                                                         |
|----------------|-----------------------------------------------------------------------------------------|
| DESCRIPTION    | Continuity Recheck Successful                                                           |
| SEVERITY       | INFO                                                                                    |
| THRESHOLD      | 100                                                                                     |
| THROTTLE       | 0                                                                                       |
| DATAWORDS      | CIC Number - TWO_BYTES<br>TGN-ID - FOUR_BYTES<br>DPC - STRING [20]<br>OPC - STRING [20] |
| PRIMARY CAUSE  | Issued when a continuity recheck of the specified CIC was successful.                   |
| PRIMARY ACTION | No action required.                                                                     |

## SIGNALING (59)

To troubleshoot and correct the cause of the alarm, refer to the [“Auto State Change for Integrated Services Digital Network Trunk Group by Media Gateway - Signaling \(59\)”](#) section on page 10-112.

|                  |                                                                                                                                                                      |
|------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| DESCRIPTION      | Auto State Change for Integrated Services Digital Network Trunk Group by Media Gateway (Auto State Change for ISDN Trunk Group by Media Gateway)                     |
| SEVERITY         | MAJOR                                                                                                                                                                |
| THRESHOLD        | 100                                                                                                                                                                  |
| THROTTLE         | 0                                                                                                                                                                    |
| DATAWORDS        | Trunk Group ID - FOUR_BYTES<br>Trunk Group Index - FOUR_BYTES<br>Media Gateway Name - STRING [65]<br>Media Gateway Index - FOUR_BYTES<br>Service Status - FOUR_BYTES |
| PRIMARY CAUSE    | Issued when the specified ISDN trunk group’s status was changed due to a media gateway operation.                                                                    |
| PRIMARY ACTION   | Monitor the event reports at the network level to determine which media gateway caused the status change of the trunk group.                                         |
| SECONDARY ACTION | Verify that the gateway is reconfigured properly to support the usage of the trunk group.                                                                            |

## SIGNALING (60)

To monitor and correct the cause of the event, refer to the [“Integrated Services Digital Network STATUS Message Containing Error Indication Received - Signaling \(60\)”](#) section on page 10-88.

|                |                                                                                                                                                                                      |
|----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| DESCRIPTION    | Integrated Services Digital Network STATUS Message Containing Error Indication Received (ISDN STATUS Message Containing Error Indication Received)                                   |
| SEVERITY       | WARNING                                                                                                                                                                              |
| THRESHOLD      | 100                                                                                                                                                                                  |
| THROTTLE       | 0                                                                                                                                                                                    |
| DATAWORDS      | Termination Name - STRING [40]<br>Termination Index - FOUR_BYTES<br>Trunk Group ID - FOUR_BYTES<br>Trunk Group Index - FOUR_BYTES<br>Cause Value - ONE_BYTE<br>Call State - ONE_BYTE |
| PRIMARY CAUSE  | Issued when an ISDN status message was received containing an error indication for the specified termination.                                                                        |
| PRIMARY ACTION | If the specified termination is not operating normally, place it in service state.                                                                                                   |

## SIGNALING (61)

For additional information, refer to the [“Trunk Operational State Changed by Service Message - Signaling \(61\)”](#) section on page 10-88.

|                |                                                                                                                                                                  |
|----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| DESCRIPTION    | Trunk Operational State Changed by Service Message                                                                                                               |
| SEVERITY       | INFO                                                                                                                                                             |
| THRESHOLD      | 100                                                                                                                                                              |
| THROTTLE       | 0                                                                                                                                                                |
| DATAWORDS      | Termination Name - STRING [40]<br>Termination Index - FOUR_BYTES<br>Trunk Group ID - FOUR_BYTES<br>Trunk Group Index - FOUR_BYTES<br>Service Status - FOUR_BYTES |
| PRIMARY CAUSE  | Issued when the specified trunk group’s operational status was changed via a service message from the specified gateway.                                         |
| PRIMARY ACTION | Monitor the event reports at the network level to verify that the specified gateway and terminations are operating normally.                                     |

## SIGNALING (62)

For additional information, refer to the [“Received Integrated Services Digital Network RESTART Message - Signaling \(62\)”](#) section on page 10-88.

|                |                                                                                                                                                        |
|----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------|
| DESCRIPTION    | Received Integrated Services Digital Network RESTART Message (Received ISDN RESTART Message)                                                           |
| SEVERITY       | INFO                                                                                                                                                   |
| THRESHOLD      | 100                                                                                                                                                    |
| THROTTLE       | 0                                                                                                                                                      |
| DATAWORDS      | Termination Name - STRING [40]<br>Termination Index - FOUR_BYTES<br>Trunk Group ID - FOUR_BYTES<br>Trunk Group Index - FOUR_BYTES<br>Flag - FOUR_BYTES |
| PRIMARY CAUSE  | Issued when an ISDN restart message was received from the specified gateway.                                                                           |
| PRIMARY ACTION | Monitor the event reports at the network level to verify that the specified gateway and terminations are operating normally.                           |

## SIGNALING (63)

To troubleshoot and correct the cause of the alarm, refer to the [“Media Gateway/Termination Faulty - Signaling \(63\)”](#) section on page 10-113.

|                |                                                                                                                                                                                                     |
|----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| DESCRIPTION    | Media Gateway/Termination Faulty                                                                                                                                                                    |
| SEVERITY       | MAJOR                                                                                                                                                                                               |
| THRESHOLD      | 100                                                                                                                                                                                                 |
| THROTTLE       | 0                                                                                                                                                                                                   |
| DATAWORDS      | Fully Qualified Name - STRING [80]<br>Type of Gateway - STRING [32]<br>Reason for Failure - STRING [80]                                                                                             |
| PRIMARY CAUSE  | Issued when a media gateway or termination has gone faulty due to the detection of an unknown endpoint, unknown package type, and unknown event, a hardware failure, or a general call agent error. |
| PRIMARY ACTION | Verify the proper operation of the media gateway specified. Place the termination out-of-service and then back into service from the call agent.                                                    |

## SIGNALING (64)

To troubleshoot and correct the cause of the alarm, refer to the [“Media Gateway Adapter Running out of Shared Memory Pools - Signaling \(64\)” section on page 10-113](#).

|                |                                                                                                                                                                                        |
|----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| DESCRIPTION    | Media Gateway Adapter Running out of Shared Memory Pools (MGA Running out of Shared Memory Pools)                                                                                      |
| SEVERITY       | CRITICAL                                                                                                                                                                               |
| THRESHOLD      | 100                                                                                                                                                                                    |
| THROTTLE       | 0                                                                                                                                                                                      |
| PRIMARY CAUSE  | Issued when the Media Gateway Control Protocol (MGCP) signaling adapter was unable to allocate data store for an inter-process communication (IPC) message due to a lack of resources. |
| PRIMARY ACTION | Call Cisco TAC technologies for assistance. (Contact Cisco TAC.)                                                                                                                       |

Refer to the [“Obtaining Technical Assistance” section on page xxxviii](#) for detailed instructions on contacting Cisco TAC and opening a service request.

## SIGNALING (65)

To troubleshoot and correct the cause of the alarm, refer to the [“Media Gateway Adapter Running out of Heap Memory - Signaling \(65\)” section on page 10-113](#).

|                |                                                                                                                                       |
|----------------|---------------------------------------------------------------------------------------------------------------------------------------|
| DESCRIPTION    | Media Gateway Adapter Running out of Heap Memory (MGA Running out of Heap Memory)                                                     |
| SEVERITY       | CRITICAL                                                                                                                              |
| THRESHOLD      | 100                                                                                                                                   |
| THROTTLE       | 0                                                                                                                                     |
| PRIMARY CAUSE  | Issued when the MGCP signaling adapter was unable to allocate data store for an IPC message from the heap due to a lack of resources. |
| PRIMARY ACTION | Call Cisco TAC Technologies for assistance. (Contact Cisco TAC.)                                                                      |

Refer to the [“Obtaining Technical Assistance” section on page xxxviii](#) for detailed instructions on contacting Cisco TAC and opening a service request.

## SIGNALING (66)

To troubleshoot and correct the cause of the alarm, refer to the [“Call Agent Internal Error \(Because of Which Media Gateway Adapter has to Start Automatically\) - Signaling \(66\)”](#) section on page 10-113.

|                |                                                                                                                                                                       |
|----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| DESCRIPTION    | Call Agent Internal Error (Because of Which Media Gateway Adapter has to Start Automatically) - (CA Internal Error (Because of Which MGA has to Start Automatically)) |
| SEVERITY       | MAJOR                                                                                                                                                                 |
| THRESHOLD      | 100                                                                                                                                                                   |
| THROTTLE       | 0                                                                                                                                                                     |
| DATAWORDS      | Fully Qualified Name - STRING [80]<br>Reason - STRING [80]<br>Detailed Reason - STRING [80]                                                                           |
| PRIMARY CAUSE  | Issued when a call agent internal error has occurred causing the restart of the MGCP signaling adapter.                                                               |
| PRIMARY ACTION | Send log files to Cisco TAC for analysis and corrective action. (Contact Cisco TAC.)                                                                                  |

Refer to the [“Obtaining Technical Assistance”](#) section on page xxxviii for detailed instructions on contacting Cisco TAC and opening a service request.



**Note**

SIGNALING (67) is not used.

## SIGNALING (68)

To troubleshoot and correct the cause of the alarm, refer to the [“Media Gateway or Termination are Found Administratively Out of Service - Signaling \(68\)”](#) section on page 10-114. For additional troubleshooting information, refer to [Appendix A, “System Usage of MGW Keepalive Parameters, Release 4.4.x.”](#)

|                |                                                                                                                                                                                             |
|----------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| DESCRIPTION    | Media Gateway or Termination are Found Administratively Out of Service                                                                                                                      |
| SEVERITY       | MAJOR                                                                                                                                                                                       |
| THRESHOLD      | 100                                                                                                                                                                                         |
| THROTTLE       | 0                                                                                                                                                                                           |
| DATAWORDS      | Fully Qualified Name - STRING [80]<br>Type of MGW- STRING [32]<br>Failure Cause - STRING [80]<br>Subscriber Info - STRING [80]<br>ICMP Ping Status - STRING [80]                            |
| PRIMARY CAUSE  | Issued when the specified media gateway is going out-of-service due to being powered down, the MGCP application going faulty, or a hardware failure.                                        |
| PRIMARY ACTION | Cycle the power on the specified media gateway. For additional troubleshooting information, refer to <a href="#">Appendix A, “System Usage of MGW Keepalive Parameters, Release 4.4.x.”</a> |

## SIGNALING (69)

To troubleshoot and correct the cause of the alarm, refer to the [“Call Agent and Feature Server Communication Message Timeout - Signaling \(69\)”](#) section on page 10-114.

|                |                                                                                                                       |
|----------------|-----------------------------------------------------------------------------------------------------------------------|
| DESCRIPTION    | Call Agent and Feature Server Communication Message Timeout (CA and FS Communication Message Timeout)                 |
| SEVERITY       | CRITICAL                                                                                                              |
| THRESHOLD      | 100                                                                                                                   |
| THROTTLE       | 0                                                                                                                     |
| DATAWORDS      | Configured CA Name - STRING [70]                                                                                      |
| PRIMARY CAUSE  | Call Agent (CA) - Feature Server (FS) communication failure due to wrong system configuration; -OR- CA or FS is down. |
| PRIMARY ACTION | Check the configuration related to CA-FS communication. FS table entries, CA entry.                                   |

## SIGNALING (70)

To monitor and correct the cause of the event, refer to the [“Integrated Services Digital Network Unable to Restore D-channel Due to Failed Communication - Signaling \(70\)”](#) section on page 10-90.

|                |                                                                                                                                                            |
|----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------|
| DESCRIPTION    | Integrated Services Digital Network Unable to Restore D-channel Due to Failed Communication (ISDN Unable to Restore D-channel Due to Failed Communication) |
| SEVERITY       | WARNING                                                                                                                                                    |
| THRESHOLD      | 100                                                                                                                                                        |
| THROTTLE       | 0                                                                                                                                                          |
| DATAWORDS      | Trunk Group ID - FOUR_BYTES<br>Trunk Group Index - FOUR_BYTES                                                                                              |
| PRIMARY CAUSE  | The ISDN signaling adapter is unable to restore a D-channel due to incorrect backhaul provisioning at the media gateway or call agent.                     |
| PRIMARY ACTION | Ensure the provisioning of the backhaul port is correct at both the call agent and media gateway.                                                          |

## SIGNALING (71)

To monitor and correct the cause of the event, refer to the [“Integrated Services Digital Network Unable to Establish D-channel - Signaling \(71\)”](#) section on page 10-90.

|                |                                                                                                                                                                                 |
|----------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| DESCRIPTION    | Integrated Services Digital Network Unable to Establish D-channel (ISDN Unable to Establish D-channel)                                                                          |
| SEVERITY       | WARNING                                                                                                                                                                         |
| THRESHOLD      | 100                                                                                                                                                                             |
| THROTTLE       | 0                                                                                                                                                                               |
| DATAWORDS      | Trunk Group ID - FOUR_BYTES<br>Trunk Group Index - FOUR_BYTES                                                                                                                   |
| PRIMARY CAUSE  | The ISDN signaling adapter is unable to establish a D-channel due to layer one parameters not being provisioned correctly or improper provisioning of the network or user side. |
| PRIMARY ACTION | Verify the correct provisioning at the media gateway.                                                                                                                           |

## SIGNALING (72)

To monitor and correct the cause of the event, refer to the [“Integrated Services Digital Network - Calls Lost Due to D-channel Down for Period of Time - Signaling \(72\)”](#) section on page 10-90.

|                |                                                                                                                                                                                                        |
|----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| DESCRIPTION    | Integrated Services Digital Network - Calls Lost Due to D-channel Down for Period of Time (ISDN - Calls Lost Due to D-channel Down for Period of Time)                                                 |
| SEVERITY       | WARNING                                                                                                                                                                                                |
| THRESHOLD      | 100                                                                                                                                                                                                    |
| THROTTLE       | 0                                                                                                                                                                                                      |
| DATAWORDS      | Trunk Group ID - FOUR_BYTES<br>Trunk Group Index - FOUR_BYTES                                                                                                                                          |
| PRIMARY CAUSE  | The ISDN signaling adapter has lost calls due to a D-channel being down as a result of a media gateway power loss or a loss of connection between the private branch exchange (PBX) and media gateway. |
| PRIMARY ACTION | Resupply power to the media gateway and verify that the connection between the PBX and media gateway is intact.                                                                                        |



## SIGNALING (73)

To monitor and correct the cause of the event, refer to the [“Integrated Services Digital Network - Unable to Send RESTART Due to RESTART Timer Expired - Signaling \(73\)”](#) section on page 10-90.

|                |                                                                                                                                                                 |
|----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| DESCRIPTION    | Integrated Services Digital Network - Unable to Send RESTART Due to RESTART Timer Expired (ISDN - Unable to Send RESTART Due to RESTART Timer Expired)          |
| SEVERITY       | WARNING                                                                                                                                                         |
| THRESHOLD      | 100                                                                                                                                                             |
| THROTTLE       | 0                                                                                                                                                               |
| DATAWORDS      | Termination Name - STRING [40]<br>Termination Index - FOUR_BYTES<br>Trunk Group ID - FOUR_BYTES<br>Trunk Group Index - FOUR_BYTES<br>Restart Class - FOUR_BYTES |
| PRIMARY CAUSE  | The ISDN signaling adapter was unable to send a RESTART message due to the expiration of the RESTART timer.                                                     |
| PRIMARY ACTION | Verify that the RESTART timer is set to an appropriate level.                                                                                                   |

## SIGNALING (74)

To monitor and correct the cause of the event, refer to the [“Integrated Services Digital Network: Unable to Send the SERVICE Due to the SERVICE Timer Expired - Signaling \(74\)”](#) section on page 10-91.

|                |                                                                                                                                                                      |
|----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| DESCRIPTION    | Integrated Services Digital Network: Unable to Send the SERVICE Due to the SERVICE Timer Expired (ISDN: Unable to Send the SERVICE Due to the SERVICE Timer Expired) |
| SEVERITY       | WARNING                                                                                                                                                              |
| THRESHOLD      | 100                                                                                                                                                                  |
| THROTTLE       | 0                                                                                                                                                                    |
| DATAWORDS      | Termination Name - STRING [40]<br>Termination Index - FOUR_BYTES<br>Trunk Group ID - FOUR_BYTES<br>Trunk Group Index - FOUR_BYTES<br>Service Status - FOUR_BYTES     |
| PRIMARY CAUSE  | The ISDN signaling adapter was unable to send a SERVICE message due to the expiration of the SERVICE timer.                                                          |
| PRIMARY ACTION | Ensure that the RESTART timer is set to an appropriate level.                                                                                                        |

## SIGNALING (75)

To troubleshoot and correct the cause of the alarm, refer to the [“Signaling System 7 Stack not Ready - Signaling \(75\)”](#) section on page 10-114.

|                  |                                                                                     |
|------------------|-------------------------------------------------------------------------------------|
| DESCRIPTION      | Signaling System 7 Stack not Ready (SS7 Stack not Ready)                            |
| SEVERITY         | CRITICAL                                                                            |
| THRESHOLD        | 100                                                                                 |
| THROTTLE         | 0                                                                                   |
| DATAWORDS        | LogicalName - STRING [64]                                                           |
| PRIMARY CAUSE    | SS7 stack not configured properly.                                                  |
| PRIMARY ACTION   | Check SS7 stack configuration.                                                      |
| SECONDARY CAUSE  | SS7 stack not ready.                                                                |
| SECONDARY ACTION | Check SS7 stack status. Do platform “ <b>start -i omni</b> ” to bring up SS7 stack. |

## SIGNALING (76)

For additional information, refer to the [“Timeout on Remote Instance - Signaling \(76\)”](#) section on page 10-91.

|                |                                                                 |
|----------------|-----------------------------------------------------------------|
| DESCRIPTION    | Timeout on Remote Instance                                      |
| SEVERITY       | INFO                                                            |
| THRESHOLD      | 100                                                             |
| THROTTLE       | 0                                                               |
| DATAWORDS      | Port Number - TWO_BYTES<br>Hostname - STRING [64]               |
| PRIMARY CAUSE  | Communication between call agent and remote instance is faulty. |
| PRIMARY ACTION | No action needed.                                               |

## SIGNALING (77)

For additional information, refer to the [“Integrated Services Digital Network D-channel Switchover for Non-Facility Associated Signaling - Signaling \(77\)”](#) section on page 10-91.

|                  |                                                                                                                                     |
|------------------|-------------------------------------------------------------------------------------------------------------------------------------|
| DESCRIPTION      | Integrated Services Digital Network D-channel Switchover for Non-Facility Associated Signaling (ISDN D-channel Switchover for NFAS) |
| SEVERITY         | INFO                                                                                                                                |
| THRESHOLD        | 100                                                                                                                                 |
| THROTTLE         | 0                                                                                                                                   |
| DATAWORDS        | Trunk Group ID - FOUR_BYTES<br>Trunk Group Index - FOUR_BYTES                                                                       |
| PRIMARY CAUSE    | Manually switched the D-channels using the command line interface (CLI).                                                            |
| PRIMARY ACTION   | Verify operator action.                                                                                                             |
| SECONDARY CAUSE  | Lost active D-channel.                                                                                                              |
| SECONDARY ACTION | Verify that gateway is operational and connection to PBX is good.                                                                   |

## SIGNALING (78)

To troubleshoot and correct the cause of the alarm, refer to the [“Integrated Services Digital Network Single D-channel Down for Non-Facility Associated Signaling - Signaling \(78\)”](#) section on page 10-114.

|                |                                                                                                                                       |
|----------------|---------------------------------------------------------------------------------------------------------------------------------------|
| DESCRIPTION    | Integrated Services Digital Network Single D-channel Down for Non-Facility Associated Signaling (ISDN Single D-channel Down for NFAS) |
| SEVERITY       | MINOR                                                                                                                                 |
| THRESHOLD      | 100                                                                                                                                   |
| THROTTLE       | 0                                                                                                                                     |
| DATAWORDS      | Trunk Group ID - FOUR_BYTES<br>Trunk Group Idx - FOUR_BYTES<br>IS Primary D Channel - FOUR_BYTES                                      |
| PRIMARY CAUSE  | One of the ISDN D-channels in primary rate interface (PRI) is down.                                                                   |
| PRIMARY ACTION | Check gateway power, and gateway connection to PBX.                                                                                   |

## SIGNALING (79)

To troubleshoot and correct the cause of the alarm, refer to the “[Media Gateway Unreachable - Signaling \(79\)](#)” section on page 10-114. For additional troubleshooting information, refer to [Appendix A, “System Usage of MGW Keepalive Parameters, Release 4.4.x.”](#)

|                |                                                                                                                                                 |
|----------------|-------------------------------------------------------------------------------------------------------------------------------------------------|
| DESCRIPTION    | Media Gateway Unreachable                                                                                                                       |
| SEVERITY       | MAJOR                                                                                                                                           |
| THRESHOLD      | 100                                                                                                                                             |
| THROTTLE       | 0                                                                                                                                               |
| DATAWORDS      | Entity Name - STRING [40]<br>General Context - STRING [40]<br>Specific Context - STRING [40]<br>Failure Context - STRING [40]                   |
| PRIMARY CAUSE  | MGCP signaling interop error has occurred.                                                                                                      |
| PRIMARY ACTION | Refer to <a href="#">Appendix A, “System Usage of MGW Keepalive Parameters, Release 4.4.x”</a> or notify customer support. (Contact Cisco TAC.) |

Refer to the “[Obtaining Technical Assistance](#)” section on page xxxviii for detailed instructions on contacting Cisco TAC and opening a service request.

## SIGNALING (80)

To troubleshoot and correct the cause of the alarm, refer to the [“Out of Bounds, Memory/Socket Error - Signaling \(80\)” section on page 10-115](#).

|                  |                                                                                                   |
|------------------|---------------------------------------------------------------------------------------------------|
| DESCRIPTION      | Out of Bounds, Memory/Socket Error                                                                |
| SEVERITY         | CRITICAL                                                                                          |
| DATAWORDS        | Process Name - STRING [40]<br>Description - STRING [40]<br>Extra Info - STRING [40]               |
| PRIMARY CAUSE    | Out of heap memory.                                                                               |
| PRIMARY ACTION   | Notify customer support. Increase random access memory (RAM). (Contact Cisco TAC.)                |
| SECONDARY CAUSE  | Out of IPC pool memory.                                                                           |
| SECONDARY ACTION | Resize IPC pool size in the platform configuration file.                                          |
| TERNARY CAUSE    | Socket error has occurred. Inappropriate/already bound socket is in use.                          |
| TERNARY ACTION   | Check UDP port supplied with media gateway adapter (MGA) command-line for validity and prior use. |

Refer to the [“Obtaining Technical Assistance” section on page xxxviii](#) for detailed instructions on contacting Cisco TAC and opening a service request.

## SIGNALING (81)

To troubleshoot and correct the cause of the alarm, refer to the [“Insufficient Heap Memory - Signaling \(81\) \(H.323\)” section on page 10-115](#).

|                |                                                                                                       |
|----------------|-------------------------------------------------------------------------------------------------------|
| DESCRIPTION    | Insufficient Heap Memory                                                                              |
| SEVERITY       | CRITICAL                                                                                              |
| THRESHOLD      | 100                                                                                                   |
| THROTTLE       | 0                                                                                                     |
| DATAWORDS      | Gateway ID - STRING [32]                                                                              |
| PRIMARY CAUSE  | Issued when the H.323 Protocol (H323) signaling adapter is unable to allocate memory from the system. |
| PRIMARY ACTION | Call CISCO TAC for assistance. (Contact Cisco TAC.)                                                   |

Refer to the [“Obtaining Technical Assistance” section on page xxxviii](#) for detailed instructions on contacting Cisco TAC and opening a service request.

## SIGNALING (82)

To troubleshoot and correct the cause of the alarm, refer to the [“Insufficient Shared Memory Pools - Signaling \(82\) \(H.323\)” section on page 10-115](#).

|                |                                                                    |
|----------------|--------------------------------------------------------------------|
| DESCRIPTION    | Insufficient Shared Memory Pools                                   |
| SEVERITY       | CRITICAL                                                           |
| THRESHOLD      | 100                                                                |
| THROTTLE       | 0                                                                  |
| DATAWORDS      | Gateway ID - STRING [32]                                           |
| PRIMARY CAUSE  | Issued when H323 signaling adapter was unable to allocate storage. |
| PRIMARY ACTION | Call Cisco TAC for corrective action. (Contact Cisco TAC.)         |

Refer to the [“Obtaining Technical Assistance” section on page xxxviii](#) for detailed instructions on contacting Cisco TAC and opening a service request.

## SIGNALING (83)

To troubleshoot and correct the cause of the alarm, refer to the [“Error While Binding to Socket - Signaling \(83\)” section on page 10-115](#).

|                |                                                                                                                 |
|----------------|-----------------------------------------------------------------------------------------------------------------|
| DESCRIPTION    | Error While Binding to Socket                                                                                   |
| SEVERITY       | CRITICAL                                                                                                        |
| THRESHOLD      | 100                                                                                                             |
| THROTTLE       | 0                                                                                                               |
| DATAWORDS      | Gateway ID - STRING [32]<br>Socket ID - FOUR_BYTES<br>Local TSAP Address - STRING [32]<br>Reason - STRING [128] |
| PRIMARY CAUSE  | An error has occurred while binding to a socket.                                                                |
| PRIMARY ACTION | Contact Cisco TAC.                                                                                              |

Refer to the [“Obtaining Technical Assistance” section on page xxxviii](#) for detailed instructions on contacting Cisco TAC and opening a service request.

## SIGNALING (84)

To troubleshoot and correct the cause of the alarm, refer to the [“Reached Maximum Socket Limit - Signaling \(84\) \(H.323\)” section on page 10-115.](#)

|                |                                                                                                        |
|----------------|--------------------------------------------------------------------------------------------------------|
| DESCRIPTION    | Reached Maximum Socket Limit                                                                           |
| SEVERITY       | CRITICAL                                                                                               |
| THRESHOLD      | 100                                                                                                    |
| THROTTLE       | 0                                                                                                      |
| DATAWORDS      | Gateway ID - STRING [32]<br>Active Sockets - FOUR_BYTES                                                |
| PRIMARY CAUSE  | The configuration setting of an H.323 signaling adapter (H3A) parameter in platform.cfg file is wrong. |
| PRIMARY ACTION | Reconfigure platform.cfg file and restart the H3A process.                                             |

## SIGNALING (85)

To troubleshoot and correct the cause of the alarm, refer to the [“Initialization Failure - Signaling \(85\)” section on page 10-116.](#)

|                |                                                                              |
|----------------|------------------------------------------------------------------------------|
| DESCRIPTION    | Initialization Failure                                                       |
| SEVERITY       | CRITICAL                                                                     |
| THRESHOLD      | 100                                                                          |
| THROTTLE       | 0                                                                            |
| DATAWORDS      | Gateway ID - STRING [32]<br>Reason - STRING [128]                            |
| PRIMARY CAUSE  | Process initialization failure has occurred.                                 |
| PRIMARY ACTION | Check Dataword 2 (Reason) for the failure cause and take action accordingly. |

## SIGNALING (86)

To troubleshoot and correct the cause of the alarm, refer to the [“Remote H323 Gateway is not Reachable - Signaling \(86\) \(H.323\)” section on page 10-116.](#)

|                |                                                                                                                               |
|----------------|-------------------------------------------------------------------------------------------------------------------------------|
| DESCRIPTION    | Remote H323 Gateway is not Reachable                                                                                          |
| SEVERITY       | MAJOR                                                                                                                         |
| THRESHOLD      | 100                                                                                                                           |
| THROTTLE       | 0                                                                                                                             |
| DATAWORDS      | Gateway ID - STRING [32]<br>Remote GW TSAP Addr - STRING [32]                                                                 |
| PRIMARY CAUSE  | Loss of communication with a remote gateway has occurred.                                                                     |
| PRIMARY ACTION | Perform standard connectivity tests - both physical checks and IP tests. Also, ensure that the gateway is not out of service. |

## SIGNALING (87)

To troubleshoot and correct the cause of the alarm, refer to the [“H323 Message Parsing Error - Signaling \(87\) \(H.323\)” section on page 10-116.](#)

|                |                                                                                                                                                                                                                                                            |
|----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| DESCRIPTION    | H323 Message Parsing Error                                                                                                                                                                                                                                 |
| SEVERITY       | MAJOR                                                                                                                                                                                                                                                      |
| THRESHOLD      | 100                                                                                                                                                                                                                                                        |
| THROTTLE       | 0                                                                                                                                                                                                                                                          |
| DATAWORDS      | Gateway ID - STRING [32]<br>Remote GW TSAP Addr - STRING [32]                                                                                                                                                                                              |
| PRIMARY CAUSE  | Unable to successfully parse an incoming H323 message.                                                                                                                                                                                                     |
| PRIMARY ACTION | This is a result of either a software bug or bad message being received - a message with a valid message type but an invalid field within the message. Snoop the message from the endpoint and verify it's content or call Cisco TAC. (Contact Cisco TAC.) |

Refer to the [“Obtaining Technical Assistance” section on page xxxviii](#) for detailed instructions on contacting Cisco TAC and opening a service request.



## SIGNALING (88)

To troubleshoot and correct the cause of the alarm, refer to the [“H323 Message Encoding Error - Signaling \(88\) \(H.323\)” section on page 10-116](#).

|                |                                                       |
|----------------|-------------------------------------------------------|
| DESCRIPTION    | H323 Message Encoding Error                           |
| SEVERITY       | MAJOR                                                 |
| THRESHOLD      | 100                                                   |
| THROTTLE       | 0                                                     |
| DATAWORDS      | Gateway ID - STRING [32]<br>Reason - STRING [128]     |
| PRIMARY CAUSE  | Unable to encode an H323 message for sending.         |
| PRIMARY ACTION | This is indicative a software bug. Contact Cisco TAC. |

Refer to the [“Obtaining Technical Assistance” section on page xxxviii](#) for detailed instructions on contacting Cisco TAC and opening a service request.

## SIGNALING (89)

To troubleshoot and correct the cause of the alarm, refer to the [“Gatekeeper not Available/Reachable - Signaling \(89\)” section on page 10-116](#).

|                |                                                                                                                                                                        |
|----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| DESCRIPTION    | Gatekeeper not Available/Reachable                                                                                                                                     |
| SEVERITY       | MAJOR                                                                                                                                                                  |
| THRESHOLD      | 100                                                                                                                                                                    |
| THROTTLE       | 0                                                                                                                                                                      |
| DATAWORDS      | Gateway ID - STRING [32]<br>Gatekeeper ID - STRING [32]<br>GK TSAP Addr - STRING [32]                                                                                  |
| PRIMARY CAUSE  | Gatekeeper is not available or is unreachable.                                                                                                                         |
| PRIMARY ACTION | Check network connectivity. Check to ensure gatekeeper (GK) is reachable by trying to ping GK IP address. If reachable, then check to ensure that GK is configured up. |

## SIGNALING (90)

To troubleshoot and correct the cause of the alarm, refer to the [“Alternate Gatekeeper is not Responding - Signaling \(90\)” section on page 10-117.](#)

|                |                                                                                                                                                                                                 |
|----------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| DESCRIPTION    | Alternate Gatekeeper is not Responding                                                                                                                                                          |
| SEVERITY       | MAJOR                                                                                                                                                                                           |
| THRESHOLD      | 100                                                                                                                                                                                             |
| THROTTLE       | 0                                                                                                                                                                                               |
| DATAWORDS      | Gateway ID - STRING [32]<br>Gatekeeper ID - STRING [32]<br>GK TSAP Addr - STRING [32]                                                                                                           |
| PRIMARY CAUSE  | Alternate gatekeeper is not responding.                                                                                                                                                         |
| PRIMARY ACTION | Check network connectivity. Check to ensure the alternate GK is reachable by trying to ping the alternate GK IP address. If reachable, then check to ensure that alternate GK is configured up. |

## SIGNALING (91)

To troubleshoot and correct the cause of the alarm, refer to the [“Endpoint Security Violation - Signaling \(91\) \(H.323\)” section on page 10-117.](#)

|                |                                                                                                                                                                                                                                                                                                                                                                                            |
|----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| DESCRIPTION    | Endpoint Security Violation                                                                                                                                                                                                                                                                                                                                                                |
| SEVERITY       | MAJOR                                                                                                                                                                                                                                                                                                                                                                                      |
| THRESHOLD      | 100                                                                                                                                                                                                                                                                                                                                                                                        |
| THROTTLE       | 0                                                                                                                                                                                                                                                                                                                                                                                          |
| DATAWORDS      | Gateway ID - STRING [32]<br>Gatekeeper ID - STRING [32]<br>GK TSAP Addr - STRING [32]                                                                                                                                                                                                                                                                                                      |
| PRIMARY CAUSE  | An H323 security violation has occurred.                                                                                                                                                                                                                                                                                                                                                   |
| PRIMARY ACTION | The password on the Cisco BTS 10200 Softswitch and/or gatekeeper is wrong - the H323 gateway (H323GW) table may not be provisioned properly OR there is a time synchronization problem between the Cisco BTS 10200 Softswitch and/or gatekeeper and the Network Time Protocol (NTP) server. Ensure both the Cisco BTS 10200 Softswitch and gatekeeper are pointing to the same NTP server. |

## SIGNALING (92)

To troubleshoot and correct the cause of the alarm, refer to the [“Invalid Call Identifier - Signaling \(92\)” section on page 10-117](#).

|                |                                                                                                                |
|----------------|----------------------------------------------------------------------------------------------------------------|
| DESCRIPTION    | Invalid Call Identifier                                                                                        |
| SEVERITY       | MINOR                                                                                                          |
| THRESHOLD      | 100                                                                                                            |
| THROTTLE       | 0                                                                                                              |
| DATAWORDS      | Gateway ID - STRING [32]<br>Remote GW TSAP Addr - STRING [32]<br>Call ID - EIGHT_BYTES                         |
| PRIMARY CAUSE  | The call ID was invalid or changed mid-call.                                                                   |
| PRIMARY ACTION | This is a software problem on the Cisco BTS 10200 Softswitch or endpoint. Call Cisco TAC. (Contact Cisco TAC.) |

Refer to the [“Obtaining Technical Assistance” section on page xxxviii](#) for detailed instructions on contacting Cisco TAC and opening a service request.

## SIGNALING (93)

To troubleshoot and correct the cause of the alarm, refer to the [“Invalid Call Reference Value - Signaling \(93\)” section on page 10-117](#).

|                |                                                                                                                        |
|----------------|------------------------------------------------------------------------------------------------------------------------|
| DESCRIPTION    | Invalid Call Reference Value                                                                                           |
| SEVERITY       | MINOR                                                                                                                  |
| THRESHOLD      | 100                                                                                                                    |
| THROTTLE       | 0                                                                                                                      |
| DATAWORDS      | Gateway ID - STRING [32]<br>Remote GW TSAP Addr - STRING [32]<br>Call ID - EIGHT_BYTES<br>Call Ref Value - EIGHT_BYTES |
| PRIMARY CAUSE  | The call ID was invalid or changed mid-call.                                                                           |
| PRIMARY ACTION | This is a software problem on the Cisco BTS 10200 Softswitch or endpoint. Call Cisco TAC. (Contact Cisco TAC.)         |

Refer to the [“Obtaining Technical Assistance” section on page xxxviii](#) for detailed instructions on contacting Cisco TAC and opening a service request.

## SIGNALING (94)

To troubleshoot and correct the cause of the alarm, refer to the [“Invalid Conference Identifier - Signaling \(94\)” section on page 10-117](#).

|                |                                                                                                                                        |
|----------------|----------------------------------------------------------------------------------------------------------------------------------------|
| DESCRIPTION    | Invalid Conference Identifier                                                                                                          |
| SEVERITY       | MINOR                                                                                                                                  |
| THRESHOLD      | 100                                                                                                                                    |
| THROTTLE       | 0                                                                                                                                      |
| DATAWORDS      | Gateway ID - STRING [32]<br>Reason - STRING [32]<br>Remote GW Port - TWO_BYTES<br>Call ID - EIGHT_BYTES<br>Conference ID - EIGHT_BYTES |
| PRIMARY CAUSE  | The call ID was invalid or changed mid-call.                                                                                           |
| PRIMARY ACTION | This is a software problem on the Cisco BTS 10200 Softswitch or endpoint. Call Cisco TAC. (Contact Cisco TAC.)                         |

Refer to the [“Obtaining Technical Assistance” section on page xxxviii](#) for detailed instructions on contacting Cisco TAC and opening a service request.

## SIGNALING (95)

To troubleshoot and correct the cause of the alarm, refer to the [“Invalid Message from the Network - Signaling \(95\)” section on page 10-118](#).

|                |                                                                                                                                                 |
|----------------|-------------------------------------------------------------------------------------------------------------------------------------------------|
| DESCRIPTION    | Invalid Message from the Network                                                                                                                |
| SEVERITY       | MINOR                                                                                                                                           |
| THRESHOLD      | 100                                                                                                                                             |
| THROTTLE       | 0                                                                                                                                               |
| DATAWORDS      | Gateway ID - STRING [32]<br>Remote GW TSAP Addr - STRING [32]<br>Call ID - EIGHT_BYTES<br>Conf ID - EIGHT_BYTES<br>Call Ref Value - EIGHT_BYTES |
| PRIMARY CAUSE  | Unsupported or invalid message type received from network.                                                                                      |
| PRIMARY ACTION | Call Cisco TAC. (Contact Cisco TAC.)                                                                                                            |

Refer to the [“Obtaining Technical Assistance” section on page xxxviii](#) for detailed instructions on contacting Cisco TAC and opening a service request.

## SIGNALING (96)

To troubleshoot and correct the cause of the alarm, refer to the [“Internal Call Processing Error - Signaling \(96\)” section on page 10-118](#).

|                |                                                                            |
|----------------|----------------------------------------------------------------------------|
| DESCRIPTION    | Internal Call Processing Error                                             |
| SEVERITY       | MINOR                                                                      |
| THRESHOLD      | 100                                                                        |
| THROTTLE       | 0                                                                          |
| DATAWORDS      | Gateway ID - STRING [32]<br>Call ID - EIGHT_BYTES<br>Reason - STRING [128] |
| PRIMARY CAUSE  | A software error has occurred.                                             |
| PRIMARY ACTION | Call Cisco TAC. (Contact Cisco TAC.)                                       |

Refer to the [“Obtaining Technical Assistance” section on page xxxviii](#) for detailed instructions on contacting Cisco TAC and opening a service request.

## SIGNALING (97)

To troubleshoot and correct the cause of the alarm, refer to the [“Insufficient Information to Complete Call - Signaling \(97\)” section on page 10-118](#).

|                |                                                                                                            |
|----------------|------------------------------------------------------------------------------------------------------------|
| DESCRIPTION    | Insufficient Information to Complete Call                                                                  |
| SEVERITY       | MINOR                                                                                                      |
| THRESHOLD      | 100                                                                                                        |
| THROTTLE       | 0                                                                                                          |
| DATAWORDS      | Gateway ID - STRING [32]<br>Call ID - EIGHT_BYTES<br>Conf ID - EIGHT_BYTES<br>Call Ref Value - EIGHT_BYTES |
| PRIMARY CAUSE  | Not enough initial call setup information was received to establish the call.                              |
| PRIMARY ACTION | Call Cisco TAC. (Contact Cisco TAC.)                                                                       |

Refer to the [“Obtaining Technical Assistance” section on page xxxviii](#) for detailed instructions on contacting Cisco TAC and opening a service request.

## SIGNALING (98)

To troubleshoot and correct the cause of the alarm, refer to the [“H323 Protocol Inconsistencies - Signaling \(98\) \(H.323\)”](#) section on page 10-118.

|                |                                                                                                                                                                     |
|----------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| DESCRIPTION    | H323 Protocol Inconsistencies                                                                                                                                       |
| SEVERITY       | MINOR                                                                                                                                                               |
| THRESHOLD      | 100                                                                                                                                                                 |
| THROTTLE       | 0                                                                                                                                                                   |
| DATAWORDS      | Gateway ID - STRING [32]<br>Call ID - EIGHT_BYTES<br>Reason - STRING [128]                                                                                          |
| PRIMARY CAUSE  | The H323 endpoint and Cisco BTS 10200 Softswitch are running different protocol versions.                                                                           |
| PRIMARY ACTION | This is only an issue where the endpoint is running a higher version of the H323 protocol than the Cisco BTS 10200 Softswitch. Call Cisco TAC. (Contact Cisco TAC.) |

Refer to the [“Obtaining Technical Assistance”](#) section on page xxxviii for detailed instructions on contacting Cisco TAC and opening a service request.

## SIGNALING (99)

To troubleshoot and correct the cause of the alarm, refer to the [“Abnormal Call Clearing - Signaling \(99\)”](#) section on page 10-118.

|                |                                                                            |
|----------------|----------------------------------------------------------------------------|
| DESCRIPTION    | Abnormal Call Clearing                                                     |
| SEVERITY       | MINOR                                                                      |
| THRESHOLD      | 100                                                                        |
| THROTTLE       | 0                                                                          |
| DATAWORDS      | Gateway ID - STRING [32]<br>Call ID - EIGHT_BYTES<br>Reason - STRING [128] |
| PRIMARY CAUSE  | Unsupported or invalid message type received from network.                 |
| PRIMARY ACTION | Call Cisco TAC. (Contact Cisco TAC.)                                       |

Refer to the [“Obtaining Technical Assistance”](#) section on page xxxviii for detailed instructions on contacting Cisco TAC and opening a service request.

## SIGNALING (100)

To troubleshoot and correct the cause of the alarm, refer to the [“Codec Negotiation Failed - Signaling \(100\)” section on page 10-119](#).

|                |                                                                                                                        |
|----------------|------------------------------------------------------------------------------------------------------------------------|
| DESCRIPTION    | Codec Negotiation Failed                                                                                               |
| SEVERITY       | MINOR                                                                                                                  |
| THRESHOLD      | 100                                                                                                                    |
| THROTTLE       | 0                                                                                                                      |
| DATAWORDS      | Gateway ID - STRING [32]<br>Call ID - EIGHT_BYTES<br>Reason - STRING [128]                                             |
| PRIMARY CAUSE  | Codec negotiation failed.                                                                                              |
| PRIMARY ACTION | Find a compatible set of codec settings for both sides, re-provision the endpoints of the call and try the call again. |

## SIGNALING (101)

To troubleshoot and correct the cause of the alarm, refer to the [“Per Call Security Violation - Signaling \(101\)” section on page 10-119](#).

|                |                                                                                  |
|----------------|----------------------------------------------------------------------------------|
| DESCRIPTION    | Per Call Security Violation                                                      |
| SEVERITY       | MINOR                                                                            |
| THRESHOLD      | 100                                                                              |
| THROTTLE       | 0                                                                                |
| DATAWORDS      | Gateway ID - STRING [32]<br>Call ID - EIGHT_BYTES<br>Gatekeeper ID - STRING [32] |
| PRIMARY CAUSE  | This is a future trap definition.                                                |
| PRIMARY ACTION | None                                                                             |

## SIGNALING (102)

To troubleshoot and correct the cause of the alarm, refer to the [“H323 Network Congested - Signaling \(102\) \(H.323\)”](#) section on page 10-119.

|                |                                                                                                                                                                                                                                                                          |
|----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| DESCRIPTION    | H323 Network Congested                                                                                                                                                                                                                                                   |
| SEVERITY       | MINOR                                                                                                                                                                                                                                                                    |
| THRESHOLD      | 100                                                                                                                                                                                                                                                                      |
| THROTTLE       | 0                                                                                                                                                                                                                                                                        |
| DATAWORDS      | Gateway ID - STRING [32]<br>Gatekeeper ID - STRING [32]                                                                                                                                                                                                                  |
| PRIMARY CAUSE  | The H323 application processes has depleted it's resources. no more calls can be completed.                                                                                                                                                                              |
| PRIMARY ACTION | The high water mark has been reached - all new call requests are rejected until the low water mark is reached. Reprovision the water marks or check the network for overload. Also verify that alternate routes have been provisioned on the Cisco BTS 10200 Softswitch. |

## SIGNALING (103)

To troubleshoot and correct the cause of the alarm, refer to the [“Aggregation Connection Down - Signaling \(103\)”](#) section on page 10-119.

|                |                                                                          |
|----------------|--------------------------------------------------------------------------|
| DESCRIPTION    | Aggregation Connection Down (AGGR Connection Down)                       |
| SEVERITY       | MAJOR                                                                    |
| THRESHOLD      | 100                                                                      |
| THROTTLE       | 0                                                                        |
| DATAWORDS      | AGGR-ID - STRING [16]                                                    |
| PRIMARY CAUSE  | Transmission Control Protocol (TCP) connection is down.                  |
| PRIMARY ACTION | Check the associated cabling and perform PINGs to test the connectivity. |



## SIGNALING (104)

For additional information, refer to the [“Aggregation Unable To Establish Connection - Signaling \(104\)” section on page 10-95](#).

|                |                                                                                  |
|----------------|----------------------------------------------------------------------------------|
| DESCRIPTION    | Aggregation Unable To Establish Connection (AGGR Unable To Establish Connection) |
| SEVERITY       | INFO                                                                             |
| THRESHOLD      | 100                                                                              |
| THROTTLE       | 0                                                                                |
| DATAWORDS      | AGGR-ID - STRING [16]                                                            |
| PRIMARY CAUSE  | TCP connection establish failure.                                                |
| PRIMARY ACTION | Check the IP connectivity of CA and cable modem termination system (CMTS).       |

## SIGNALING (105)

For additional information, refer to the [“Aggregation Gate Set Failed - Signaling \(105\)” section on page 10-95](#).

|                |                                                                               |
|----------------|-------------------------------------------------------------------------------|
| DESCRIPTION    | Aggregation Gate Set Failed (AGGR Gate Set Failed)                            |
| SEVERITY       | INFO                                                                          |
| THRESHOLD      | 100                                                                           |
| THROTTLE       | 0                                                                             |
| DATAWORDS      | AGGR-ID - STRING [16]<br>Error-Code - TWO_BYTES<br>Sub-Error-Code - TWO_BYTES |
| PRIMARY CAUSE  | Gate set acknowledgement never came from the CMTS.                            |
| PRIMARY ACTION | None                                                                          |

## SIGNALING (106)

To troubleshoot and correct the cause of the alarm, refer to the [“Enhanced Subscriber Authentication Cisco BTS 10200 Softswitch Delivery Function Connection Down - Signaling \(106\)”](#) section on page 10-119.

|                |                                                                                                                              |
|----------------|------------------------------------------------------------------------------------------------------------------------------|
| DESCRIPTION    | Enhanced Subscriber Authentication Cisco BTS 10200 Softswitch Delivery Function Connection Down (ESA BTS DF Connection Down) |
| SEVERITY       | MINOR                                                                                                                        |
| THRESHOLD      | 100                                                                                                                          |
| THROTTLE       | 0                                                                                                                            |
| PRIMARY CAUSE  | Delivery function (DF) server not responding.                                                                                |
| PRIMARY ACTION | Check the encryption key or IP connectivity to DF.                                                                           |

## SIGNALING (107)

To troubleshoot and correct the cause of the alarm, refer to the [“Logical Internet Protocol Addresses not Mapped Correctly - Signaling \(107\)”](#) section on page 10-120.

|                   |                                                                                                                                   |
|-------------------|-----------------------------------------------------------------------------------------------------------------------------------|
| DESCRIPTION       | Logical Internet Protocol Addresses not Mapped Correctly (Logical IP Addresses not Mapped Correctly)                              |
| SEVERITY          | CRITICAL                                                                                                                          |
| THRESHOLD         | 30                                                                                                                                |
| THROTTLE          | 0                                                                                                                                 |
| DATAWORDS         | Contact Domain Name - STRING [128]<br>Number of IP Addresses Resolved - FOUR_BYTES<br>Number of Virtual IP Addresses - FOUR_BYTES |
| PRIMARY CAUSE     | Contact name in the configuration file not configured in domain name system (DNS).                                                |
| PRIMARY ACTION    | Verify name in DNS matches name in platform.cfg and opticall.cfg files.                                                           |
| SECONDARY CAUSE   | Contact could not be resolved to an IP address on the host.                                                                       |
| SECONDARY ACTION  | Verify DNS resolves to IP addresses reserved for process on the Cisco BTS 10200 Softswitch.                                       |
| TERNARY CAUSE     | IP address manager not running.                                                                                                   |
| TERNARY ACTION    | Verify Internet Protocol Manager (IPM) process is running and check for alarms from IPM.                                          |
| SUBSEQUENT CAUSE  | Mis-configuration during installation or manual changes made after installation.                                                  |
| SUBSEQUENT ACTION | Contact Cisco TAC for support. (Contact Cisco TAC.)                                                                               |

Refer to the [“Obtaining Technical Assistance”](#) section on page xxxviii for detailed instructions on contacting Cisco TAC and opening a service request.

## SIGNALING (108)

To troubleshoot and correct the cause of the alarm, refer to the [“Current SIA Configuration only Valid for Simplex Systems - Signaling \(108\)”](#) section on page 10-120.

|                  |                                                                                               |
|------------------|-----------------------------------------------------------------------------------------------|
| DESCRIPTION      | Current SIA Configuration only Valid for Simplex Systems                                      |
| SEVERITY         | MAJOR                                                                                         |
| THRESHOLD        | 100                                                                                           |
| THROTTLE         | 0                                                                                             |
| DATAWORDS        | SIA Host Domain Name - STRING [128]<br>SIA Contact Domain N - STRING [128]                    |
| PRIMARY CAUSE    | SIA host and contact parameters are the same in platform.cfg file.                            |
| PRIMARY ACTION   | If this is a duplex installation, regardless of current operational state, contact Cisco TAC. |
| SECONDARY CAUSE  | SIA is configured for use on a simplex system.                                                |
| SECONDARY ACTION | If this is a simplex installation only, this alarm can be turned off.                         |

Refer to the [“Obtaining Technical Assistance”](#) section on page xxxviii for detailed instructions on contacting Cisco TAC and opening a service request.

## SIGNALING (109)

To troubleshoot and correct the cause of the alarm, refer to the [“Stream Control Transmission Protocol Association Failure - Signaling \(109\)”](#) section on page 10-121.

|                  |                                                                                     |
|------------------|-------------------------------------------------------------------------------------|
| DESCRIPTION      | Stream Control Transmission Protocol Association Failure (SCTP Association Failure) |
| SEVERITY         | MAJOR                                                                               |
| THRESHOLD        | 100                                                                                 |
| THROTTLE         | 0                                                                                   |
| DATAWORDS        | SCTP Association ID - STRING [17]                                                   |
| PRIMARY CAUSE    | Ethernet cables on signaling gateway process (SGP) are unplugged or severed.        |
| PRIMARY ACTION   | Plug Ethernet cables in or fix severed connection.                                  |
| SECONDARY CAUSE  | SGP is not operational.                                                             |
| SECONDARY ACTION | Check SGP alarms to determine why it is not operating properly.                     |

## SIGNALING (110)

To troubleshoot and correct the cause of the alarm, refer to the [“Signaling Gateway Group Is Out-of-Service - Signaling \(110\)”](#) section on page 10-125.

|                  |                                                                                                                                |
|------------------|--------------------------------------------------------------------------------------------------------------------------------|
| DESCRIPTION      | Signaling Gateway Group is Out-of-Service                                                                                      |
| SEVERITY         | CRITICAL                                                                                                                       |
| THRESHOLD        | 100                                                                                                                            |
| THROTTLE         | 0                                                                                                                              |
| DATAWORDS        | SG Group ID - STRING [17]                                                                                                      |
| PRIMARY CAUSE    | All Stream Control Transmission Protocol (SCTP) associations between CA and SGs are out-of-service.                            |
| PRIMARY ACTION   | Make sure all Ethernet connections on the CA and SGs are plugged in. Also make sure all associated IP routers are operational. |
| SECONDARY CAUSE  | The MTP3 user adapter (M3UA) layer is down between the CA and SGs.                                                             |
| SECONDARY ACTION | Use Cisco Snooper application to determine why the M3UA layer is down.                                                         |

## SIGNALING (111)

To troubleshoot and correct the cause of the alarm, refer to the [“Stream Control Transmission Protocol Association Degraded \(One of Two Internet Protocol Connections Down\) - Signaling \(111\)”](#) section on page 10-125.

|                  |                                                                                                                                                                        |
|------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| DESCRIPTION      | Stream Control Transmission Protocol Association Degraded (One of Two Internet Protocol Connections Down) (SCTP Association Degraded (One of Two IP connections Down)) |
| SEVERITY         | MAJOR                                                                                                                                                                  |
| THRESHOLD        | 100                                                                                                                                                                    |
| THROTTLE         | 0                                                                                                                                                                      |
| DATAWORDS        | SCTP Association ID - STRING [17]<br>Destination IP Address - STRING [11]                                                                                              |
| PRIMARY CAUSE    | Single Ethernet connection on CA or SGP is unplugged or severed.                                                                                                       |
| PRIMARY ACTION   | Plug in all Ethernet connections or repair if severed.                                                                                                                 |
| SECONDARY CAUSE  | SCTP communication problem - protocol timeout.                                                                                                                         |
| SECONDARY ACTION | Use Cisco Snooper application to determine why SCTP association is degraded.                                                                                           |

## SIGNALING (112)

To troubleshoot and correct the cause of the alarm, refer to the [“Stream Control Transmission Protocol Association Configuration Error - Signaling \(112\)”](#) section on page 10-126.

|                  |                                                                                                             |
|------------------|-------------------------------------------------------------------------------------------------------------|
| DESCRIPTION      | Stream Control Transmission Protocol Association Configuration Error (SCTP Association Configuration Error) |
| SEVERITY         | MINOR                                                                                                       |
| THRESHOLD        | 100                                                                                                         |
| THROTTLE         | 0                                                                                                           |
| DATAWORDS        | SCTP Association ID - STRING [17]                                                                           |
| PRIMARY CAUSE    | Destination IP address is invalid.                                                                          |
| PRIMARY ACTION   | Input new destination IP address - see log for additional details.                                          |
| SECONDARY CAUSE  | Local IP address is invalid.                                                                                |
| SECONDARY ACTION | Input new local IP address information.                                                                     |
| TERNARY CAUSE    | IP Routing Table is not configured properly.                                                                |
| TERNARY ACTION   | Have the system administrator configure IP routing table.                                                   |

## SIGNALING (113)

To troubleshoot and correct the cause of the alarm, refer to the [“Signaling Gateway Failure - Signaling \(113\)”](#) section on page 10-126.

|                |                                                                                 |
|----------------|---------------------------------------------------------------------------------|
| DESCRIPTION    | Signaling Gateway Failure                                                       |
| SEVERITY       | MAJOR                                                                           |
| THRESHOLD      | 100                                                                             |
| THROTTLE       | 0                                                                               |
| DATAWORDS      | Signaling Gateway ID - STRING [17]                                              |
| PRIMARY CAUSE  | All associated signaling gateway processes are out-of-service.                  |
| PRIMARY ACTION | Determine why each associated SGP is out-of-service (see SGP alarm definition). |

## SIGNALING (114)

To troubleshoot and correct the cause of the alarm, refer to the [“Signaling Gateway Process Is Out-of-Service - Signaling \(114\)” section on page 10-127](#).

|                  |                                                                                                       |
|------------------|-------------------------------------------------------------------------------------------------------|
| DESCRIPTION      | Signaling Gateway Process is Out-of-Service                                                           |
| SEVERITY         | MAJOR                                                                                                 |
| THRESHOLD        | 100                                                                                                   |
| THROTTLE         | 0                                                                                                     |
| DATAWORDS        | Signaling Gateway - STRING [17]                                                                       |
| PRIMARY CAUSE    | All SCTP associations between the SGP and the CA are out-of-service.                                  |
| PRIMARY ACTION   | See SCTP association alarm definition to determine how to rectify the problem.                        |
| SECONDARY CAUSE  | The M3UA layer is down between the CA and SGP.                                                        |
| SECONDARY ACTION | Use Cisco snoop utility to determine why M3UA layer is down. Also see log for additional information. |

## SIGNALING (115)

To monitor and correct the cause of the event, refer to the [“Invalid Routing Context Received - Signaling \(115\)” section on page 10-97](#).

|                |                                                                            |
|----------------|----------------------------------------------------------------------------|
| DESCRIPTION    | Invalid Routing Context Received                                           |
| SEVERITY       | WARNING                                                                    |
| THRESHOLD      | 100                                                                        |
| THROTTLE       | 0                                                                          |
| DATAWORDS      | Invalid Routing Cont - FOUR_BYTES<br>SG from Which the In - STRING [17]    |
| PRIMARY CAUSE  | Routing context was configured improperly on CA or signaling gateway (SG). |
| PRIMARY ACTION | Reconfigure routing context on CA or SG so that they match in both places. |

## SIGNALING (116)

To troubleshoot and correct the cause of the alarm, refer to the [“Destination Point Code User Part Unavailable - Signaling \(116\)”](#) section on page 10-127.

|                |                                                                                                                                |
|----------------|--------------------------------------------------------------------------------------------------------------------------------|
| DESCRIPTION    | Destination Point Code User Part Unavailable (DPC User Part Unavailable)                                                       |
| SEVERITY       | MAJOR                                                                                                                          |
| THRESHOLD      | 100                                                                                                                            |
| THROTTLE       | 0                                                                                                                              |
| DATAWORDS      | DPC ID - STRING [17]                                                                                                           |
| PRIMARY CAUSE  | SGP sent a destination user part unavailable (DUPU) M3UA message to CA indicating that a User Part is unavailable on at a DPC. |
| PRIMARY ACTION | Contact SS7 Network Administrator to report the User Part Unavailable problem of the DPC so communication can be restored.     |

## SIGNALING (117)

To troubleshoot and correct the cause of the alarm, refer to the [“Circuit Validation Test Message Received for an Unequipped Circuit Identification Code - Signaling \(117\)”](#) section on page 10-127.

|                |                                                                                                                                     |
|----------------|-------------------------------------------------------------------------------------------------------------------------------------|
| DESCRIPTION    | Circuit Validation Test Message Received for an Unequipped Circuit Identification Code (CVT Message Received for an Unequipped CIC) |
| SEVERITY       | MINOR                                                                                                                               |
| THRESHOLD      | 100                                                                                                                                 |
| THROTTLE       | 0                                                                                                                                   |
| DATAWORDS      | CIC - TWO_BYTES<br>TGN-ID - EIGHT_BYTES<br>DPC - STRING [13]                                                                        |
| PRIMARY CAUSE  | CIC is not provisioned                                                                                                              |
| PRIMARY ACTION | Provision CIC.                                                                                                                      |



## SIGNALING (118)

To troubleshoot and correct the cause of the alarm, refer to the [“Circuit Verification Response Received with Failed Indication - Signaling \(118\)”](#) section on page 10-127.

|                |                                                                                                                            |
|----------------|----------------------------------------------------------------------------------------------------------------------------|
| DESCRIPTION    | Circuit Verification Response Received with Failed Indication (CVR Received with Failed Indication)                        |
| SEVERITY       | MINOR                                                                                                                      |
| THRESHOLD      | 100                                                                                                                        |
| THROTTLE       | 0                                                                                                                          |
| DATAWORDS      | CIC - TWO_BYTES<br>TGN-ID - EIGHT_BYTES<br>DPC - STRING [20]<br>OPC - STRING [20]                                          |
| PRIMARY CAUSE  | CIC mismatch.                                                                                                              |
| PRIMARY ACTION | Perform internal test such as checking that the CIC is assigned to a circuit between the sending and the receiving switch. |

## SIGNALING (119)

To troubleshoot and correct the cause of the alarm, refer to the [“Signaling System 7 Adapter Process Faulty - Signaling \(119\)”](#) section on page 10-127.

|                |                                                                                         |
|----------------|-----------------------------------------------------------------------------------------|
| DESCRIPTION    | Signaling System 7 Adapter Process Faulty (S7A Process Faulty)                          |
| SEVERITY       | CRITICAL                                                                                |
| THRESHOLD      | 100                                                                                     |
| THROTTLE       | 0                                                                                       |
| DATAWORDS      | Reason - STRING [36]                                                                    |
| PRIMARY CAUSE  | OMNI or S7A exception.                                                                  |
| PRIMARY ACTION | Check OMNI process. The S7A will restart itself if S7A maximum restart is not exceeded. |

## SIGNALING (120)

To troubleshoot and correct the cause of the alarm, refer to the [“Signaling System 7 Module/Signaling System 7 Adapter Faulty - Signaling \(120\)”](#) section on page 10-128.

|                |                                                                              |
|----------------|------------------------------------------------------------------------------|
| DESCRIPTION    | Signaling System 7 Module/Signaling System 7 Adapter Faulty (S7M/S7A Faulty) |
| SEVERITY       | CRITICAL                                                                     |
| THRESHOLD      | 100                                                                          |
| THROTTLE       | 0                                                                            |
| DATAWORDS      | Reason - STRING [36]                                                         |
| PRIMARY CAUSE  | OMNI failure.                                                                |
| PRIMARY ACTION | Check OMNI status; failover will occur in a duplex configuration.            |

## SIGNALING (121)

To troubleshoot and correct the cause of the alarm, refer to the [“Message Transfer Part 3 User Adapter Cannot Go Standby - Signaling \(121\)”](#) section on page 10-128.

|                |                                                                                                                                  |
|----------------|----------------------------------------------------------------------------------------------------------------------------------|
| DESCRIPTION    | Message Transfer Part 3 User Adapter Cannot Go Standby (M3UA/SUA Cannot Go Standby)                                              |
| SEVERITY       | MAJOR                                                                                                                            |
| THRESHOLD      | 100                                                                                                                              |
| THROTTLE       | 0                                                                                                                                |
| DATAWORDS      | Platform ID - STRING [17]                                                                                                        |
| PRIMARY CAUSE  | No INACTIVE acknowledge (ACK) messages received from any SG or SCTP Associations are probably down.                              |
| PRIMARY ACTION | Investigate other alarms to see if SGs are down or SCTP associations are down. Take corrective action according to those alarms. |

## SIGNALING (122)

To troubleshoot and correct the cause of the alarm, refer to the [“Message Transfer Part 3 User Adapter Cannot Go Active - Signaling \(122\)”](#) section on page 10-128.

|                |                                                                                                                                  |
|----------------|----------------------------------------------------------------------------------------------------------------------------------|
| DESCRIPTION    | Message Transfer Part 3 User Adapter Cannot Go Active (M3UA/SUA Cannot Go Active)                                                |
| SEVERITY       | MAJOR                                                                                                                            |
| THRESHOLD      | 100                                                                                                                              |
| THROTTLE       | 0                                                                                                                                |
| DATAWORDS      | Platform ID - STRING [17]                                                                                                        |
| PRIMARY CAUSE  | No ACTIVE acknowledgement messages received from any SG or SCTP associations are probably down.                                  |
| PRIMARY ACTION | Investigate other alarms to see if SGs are down or SCTP associations are down. Take corrective action according to those alarms. |



### Note

SIGNALING (123) is not used.

## SIGNALING (124)

To troubleshoot and correct the cause of the alarm, refer to the [“Remote Subsystem is Out Of Service - Signaling \(124\)”](#) section on page 10-128.

|                |                                                                        |
|----------------|------------------------------------------------------------------------|
| DESCRIPTION    | Remote Subsystem is Out Of Service                                     |
| SEVERITY       | MINOR                                                                  |
| THRESHOLD      | 100                                                                    |
| THROTTLE       | 0                                                                      |
| DATAWORDS      | Destination Point Co - STRING [20]<br>Remote Subsystem Num - TWO_BYTES |
| PRIMARY CAUSE  | Link loss or the remote subsystem out of service.                      |
| PRIMARY ACTION | Check links. Check remote location, if possible.                       |

## SIGNALING (125)

To troubleshoot and correct the cause of the alarm, refer to the [“Signaling Connection Control Part Routing Error - Signaling \(125\)” section on page 10-129.](#)

|                |                                                                          |
|----------------|--------------------------------------------------------------------------|
| DESCRIPTION    | Signaling Connection Control Part Routing Error (SCCP Routing Error)     |
| SEVERITY       | MAJOR                                                                    |
| THRESHOLD      | 100                                                                      |
| THROTTLE       | 0                                                                        |
| PRIMARY CAUSE  | Signaling connection control part (SCCP) route invalid or not available. |
| PRIMARY ACTION | Provision the right SCCP route.                                          |

## SIGNALING (126)

To troubleshoot and correct the cause of the alarm, refer to the [“Signaling Connection Control Part Binding Failure - Signaling \(126\)” section on page 10-129.](#)

|                |                                                                                                                                                 |
|----------------|-------------------------------------------------------------------------------------------------------------------------------------------------|
| DESCRIPTION    | Signaling Connection Control Part Binding Failure (SCCP Binding Failure)                                                                        |
| SEVERITY       | MAJOR                                                                                                                                           |
| THRESHOLD      | 100                                                                                                                                             |
| THROTTLE       | 0                                                                                                                                               |
| DATAWORDS      | Local Point Code - STRING [20]<br>Local Subsystem Numb - ONE_BYTE                                                                               |
| PRIMARY CAUSE  | Trillium stack binding failure.                                                                                                                 |
| PRIMARY ACTION | Re-initialize the TCAP signaling adapter (TSA) process or remove the subsystem from the Element Management System (EMS) table and add it again. |

## SIGNALING (127)

To troubleshoot and correct the cause of the alarm, refer to the [“Transaction Capabilities Application Part Binding Failure - Signaling \(127\)” section on page 10-129.](#)

|                |                                                                                            |
|----------------|--------------------------------------------------------------------------------------------|
| DESCRIPTION    | Transaction Capabilities Application Part Binding Failure (TCAP Binding Failure)           |
| SEVERITY       | MAJOR                                                                                      |
| THRESHOLD      | 100                                                                                        |
| THROTTLE       | 0                                                                                          |
| PRIMARY CAUSE  | Trillium stack binding failure.                                                            |
| PRIMARY ACTION | Re-initialize the TSA process or remove the subsystem from the EMS table and add it again. |

**Note**

SIGNALING (128) through SIGNALING (131) are not used.

## SIGNALING (132)

To monitor and correct the cause of the event, refer to the [“Transaction Capabilities Application Part Reaches the Provisioned Resource Limit - Signaling \(132\)”](#) section on page 10-99.

|               |                                                                                                                                |
|---------------|--------------------------------------------------------------------------------------------------------------------------------|
| DESCRIPTION   | Transaction Capabilities Application Part Reaches the Provisioned Resource Limit (TCAP Reaches the Provisioned Resource Limit) |
| SEVERITY      | WARNING                                                                                                                        |
| THRESHOLD     | 100                                                                                                                            |
| THROTTLE      | 0                                                                                                                              |
| DATAWORDS     | Dialogue/Invoke ID - FOUR_BYTES                                                                                                |
| PRIMARY CAUSE | Transaction Capabilities Application Part (TCAP) runs out of all the pre-configured dialogue IDs or invoke IDs.                |

## SIGNALING (133)

For additional information, refer to the [“Unable to Decode Generic Transport Descriptor Message - Signaling \(133\)”](#) section on page 10-99.

|                  |                                                                                                                                                  |
|------------------|--------------------------------------------------------------------------------------------------------------------------------------------------|
| DESCRIPTION      | Unable to Decode Generic Transport Descriptor Message (Unable to Decode GTD Message)                                                             |
| SEVERITY         | INFO                                                                                                                                             |
| THRESHOLD        | 100                                                                                                                                              |
| THROTTLE         | 0                                                                                                                                                |
| DATAWORDS        | Endpoint Name - STRING [40]<br>GTD Content Type - STRING [40]                                                                                    |
| PRIMARY CAUSE    | Issued when the generic transport descriptor (GTD) parser failed to decode a GTD message received from the specified endpoint.                   |
| PRIMARY ACTION   | Verify that the version of the GTD protocol used by the device at the remote endpoint is consistent with the version expected by the call agent. |
| SECONDARY ACTION | Examine the associated signaling link to see if there is any interruption of the supplementary services on the link.                             |

## SIGNALING (134)

For additional information, refer to the [“Signaling System 7 Message Encoding Failure - Signaling \(134\)” section on page 10-100.](#)

|                |                                                                                         |
|----------------|-----------------------------------------------------------------------------------------|
| DESCRIPTION    | Signaling System 7 Message Encoding Failure (SS7 Message Encoding Failure)              |
| SEVERITY       | INFO                                                                                    |
| THRESHOLD      | 100                                                                                     |
| THROTTLE       | 0                                                                                       |
| DATAWORDS      | CIC Number - TWO_BYTES<br>TGN-ID - FOUR_BYTES<br>DPC - STRING [20]<br>OPC - STRING [20] |
| PRIMARY CAUSE  | Error in ISDN user part (ISUP) stack or signaling adapter interface (SAI) message.      |
| PRIMARY ACTION | Capture SS7 trace of circuit for examination by support personnel. (Contact Cisco TAC.) |

Refer to the [“Obtaining Technical Assistance” section on page xxxviii](#) for detailed instructions on contacting Cisco TAC and opening a service request.

## SIGNALING (135)

For additional information, refer to the [“Signaling System 7 Message Decoding Failure - Signaling \(135\)” section on page 10-100.](#)

|                |                                                                                         |
|----------------|-----------------------------------------------------------------------------------------|
| DESCRIPTION    | Signaling System 7 Message Decoding Failure (SS7 Message Decoding Failure)              |
| SEVERITY       | INFO                                                                                    |
| THRESHOLD      | 100                                                                                     |
| THROTTLE       | 0                                                                                       |
| DATAWORDS      | CIC Number - TWO_BYTES<br>TGN-ID - FOUR_BYTES<br>DPC - STRING [20]<br>OPC - STRING [20] |
| PRIMARY CAUSE  | Error in ISUP stack or SAI message.                                                     |
| PRIMARY ACTION | Capture SS7 trace of circuit for examination by support personnel. (Contact Cisco TAC.) |

Refer to the [“Obtaining Technical Assistance” section on page xxxviii](#) for detailed instructions on contacting Cisco TAC and opening a service request.

## SIGNALING (136)

For additional information, refer to the [“Signaling System 7 Message Invalid Received - Signaling \(136\)” section on page 10-100](#).

|                  |                                                                                                |
|------------------|------------------------------------------------------------------------------------------------|
| DESCRIPTION      | Signaling System 7 Message Invalid Received (SS7 Message Invalid Received)                     |
| SEVERITY         | INFO                                                                                           |
| THRESHOLD        | 100                                                                                            |
| THROTTLE         | 0                                                                                              |
| DATAWORDS        | CIC Number - TWO_BYTES<br>TGN-ID - FOUR_BYTES<br>DPC - STRING [20]<br>OPC - STRING [20]        |
| PRIMARY CAUSE    | Invalid message was received from line in ISUP stack.                                          |
| PRIMARY ACTION   | Capture SS7 trace of circuit for examination by support personnel. (Contact Cisco TAC.)        |
| SECONDARY CAUSE  | Invalid message was received from line in ISUP stack.                                          |
| SECONDARY ACTION | Verify the signal switching point (SSP) sending the message to the CA is correctly configured. |

Refer to the [“Obtaining Technical Assistance” section on page xxxviii](#) for detailed instructions on contacting Cisco TAC and opening a service request.

## SIGNALING (137)

For additional information, refer to the [“Signaling System 7 Confusion Message Received - Signaling \(137\)” section on page 10-100](#).

|                |                                                                                                                                                                                                                                                                                                        |
|----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| DESCRIPTION    | Signaling System 7 Confusion Message Received (SS7 Confusion Message Received)                                                                                                                                                                                                                         |
| SEVERITY       | INFO                                                                                                                                                                                                                                                                                                   |
| THRESHOLD      | 100                                                                                                                                                                                                                                                                                                    |
| THROTTLE       | 0                                                                                                                                                                                                                                                                                                      |
| DATAWORDS      | CIC Number - TWO_BYTES<br>TGN-ID - FOUR_BYTES<br>DPC - STRING [20]<br>OPC - STRING [20]                                                                                                                                                                                                                |
| PRIMARY CAUSE  | An ISUP message or parameter received was not recognized or understood.                                                                                                                                                                                                                                |
| PRIMARY ACTION | Check the log for more information (including confusion (CFN) diagnostic output). Capture SS7 trace of affected circuits. If diagnostic data indicates messages/parameters that must be supported are being dropped, refer the captured data to support along with a description of the call scenario. |

## SIGNALING (138)

To troubleshoot and correct the cause of the alarm, refer to the [“Number of Open Session Initiation Protocol Connections is Reaching Engineered Limit - Signaling \(138\)”](#) section on page 129.

|                |                                                                                                                                                                                        |
|----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| DESCRIPTION    | Number of Open Session Initiation Protocol Connections is Reaching Engineered Limit (Number of Open SIP Connections is Reaching Engineered Limit)                                      |
| SEVERITY       | MINOR                                                                                                                                                                                  |
| THRESHOLD      | 100                                                                                                                                                                                    |
| THROTTLE       | 0                                                                                                                                                                                      |
| DATAWORDS      | Number of SIP Connections Open - FOUR_BYTES<br>SIP Connection Alarm Threshold - FOUR_BYTES<br>Open SIP Connection Limit - FOUR_BYTES                                                   |
| PRIMARY CAUSE  | System configuration and traffic load have caused the number of open connections to approach the engineered limit. This limit will need to be increased to allow for more connections. |
| PRIMARY ACTION | Please contact Cisco support. (Contact Cisco TAC.)                                                                                                                                     |

Refer to the [“Obtaining Technical Assistance”](#) section on page xxxviii for detailed instructions on contacting Cisco TAC and opening a service request.

## SIGNALING (139)

For additional information, refer to the [“Signaling System 7 Trunk was Found to be in Erroneous State - Signaling \(139\) \(SS7\)”](#) section on page 10-101.

|                |                                                                                                                                                                                    |
|----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| DESCRIPTION    | Signaling System 7 Trunk was Found to be in Erroneous State (SS7 Trunk was Found to be in Erroneous State)                                                                         |
| SEVERITY       | INFO                                                                                                                                                                               |
| THRESHOLD      | 100                                                                                                                                                                                |
| THROTTLE       | 0                                                                                                                                                                                  |
| DATAWORDS      | CIC - TWO_BYTES<br>TGN-ID - FOUR_BYTES<br>DPC - STRING [20]<br>OPC - STRING [20]<br>Near-End State - STRING [64]<br>Far-End State - STRING [64]<br>Resolution Action - STRING [64] |
| PRIMARY CAUSE  | Discrepancy between local and remote trunk states.                                                                                                                                 |
| PRIMARY ACTION | Automatic corrective action enforced when using American National Standards Institute (ANSI) ISUP.                                                                                 |



## SIGNALING (140)

For additional information, refer to the “[Unanswered Information Message - Signaling \(140\)](#)” section on [page 10-101](#).

|                |                                                                                                          |
|----------------|----------------------------------------------------------------------------------------------------------|
| DESCRIPTION    | Unanswered Information Message (Unanswered INF Message)                                                  |
| SEVERITY       | INFO                                                                                                     |
| THRESHOLD      | 100                                                                                                      |
| THROTTLE       | 0                                                                                                        |
| DATAWORDS      | CIC - TWO_BYTES<br>TGN-ID - FOUR_BYTES<br>DPC - STRING [20]<br>OPC - STRING [20]                         |
| PRIMARY CAUSE  | Far-end switch is not responding to information (INF) message with an information request (INR) message. |
| PRIMARY ACTION | Verify that far-end switch can correctly respond to an INF message.                                      |

## SIGNALING (141)

To monitor and correct the cause of the event, refer to the “[Address not Resolved by Domain Name System Server - Signaling \(141\)](#)” section on [page 10-101](#).

|                |                                                                                           |
|----------------|-------------------------------------------------------------------------------------------|
| DESCRIPTION    | Address not Resolved by Domain Name System Server (Address not Resolved by DNS Server)    |
| SEVERITY       | WARNING                                                                                   |
| THRESHOLD      | 100                                                                                       |
| THROTTLE       | 0                                                                                         |
| DATAWORDS      | TSAP_Address/Hostname - STRING [256]                                                      |
| PRIMARY CAUSE  | The transport service access point (TSAP) address/hostname is not defined in DNS.         |
| PRIMARY ACTION | Add entry for TSAP address to DNS server, or fix Cisco BTS 10200 Softswitch provisioning. |

## SIGNALING (142)

To troubleshoot and correct the cause of the alarm, refer to the [“Session Initiation Protocol Trunk Operationally Out-of-Service - Signaling \(142\)”](#) section on page 10-129.

|                  |                                                                                                                                                                                                                                                                                                                                                            |
|------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| DESCRIPTION      | Session Initiation Protocol Trunk Operationally Out-of-Service (SIP Trunk Operationally out of Service)                                                                                                                                                                                                                                                    |
| SEVERITY         | CRITICAL                                                                                                                                                                                                                                                                                                                                                   |
| THRESHOLD        | 100                                                                                                                                                                                                                                                                                                                                                        |
| THROTTLE         | 0                                                                                                                                                                                                                                                                                                                                                          |
| DATAWORDS        | Trunk Group Description - STRING [16]<br>Trunk TSAP Address - STRING [65]                                                                                                                                                                                                                                                                                  |
| PRIMARY CAUSE    | Issued when Cisco BTS 10200 Softswitch is unable to communicate with a remote SIP party (Call-Agent or Proxy) over a SIP or SIP-T trunk.                                                                                                                                                                                                                   |
| PRIMARY ACTION   | Verify DNS resolution exists, if TSAP address of the remote entity is a domain name. Verify the remote entity is reachable by Internet Control Message Protocol (ICMP) ping, using the Trunk TSAP address from the Event Report. If the same alarm is reported on all the softswitch trunk groups, then verify that the network connection is operational. |
| SECONDARY CAUSE  | Remote SIP party is not operational.                                                                                                                                                                                                                                                                                                                       |
| SECONDARY ACTION | If the ping is not successful, then diagnose the issue that prevents the TSAP address from being reached. Verify the SIP application is running on the remote host and listening on the port specified in the TSAP address.                                                                                                                                |

## SIGNALING (143)

To troubleshoot and correct the cause of the alarm, refer to the [“Internet Protocol Interface Link to the Signaling System 7 Signaling Gateway is Down - Signaling \(143\)”](#) section on page 10-130.

|                |                                                                                                                                               |
|----------------|-----------------------------------------------------------------------------------------------------------------------------------------------|
| DESCRIPTION    | Internet Protocol Interface Link to the Signaling System 7 Signaling Gateway is Down (IP Interface Link to the SS7 Signaling Gateway is Down) |
| SEVERITY       | MINOR                                                                                                                                         |
| THRESHOLD      | 100                                                                                                                                           |
| THROTTLE       | 0                                                                                                                                             |
| DATAWORDS      | Interface Name - STRING [65]<br>Interface IP Address - STRING [65]                                                                            |
| PRIMARY CAUSE  | Hardware problem has occurred.                                                                                                                |
| PRIMARY ACTION | Check the link interfaces.                                                                                                                    |

## SIGNALING (144)

To troubleshoot and correct the cause of the alarm, refer to the [“All Internet Protocol Interface Links to Signaling System 7 Signaling Gateway are Down - Signaling \(144\)”](#) section on page 10-130.

|                |                                                                                                                                                   |
|----------------|---------------------------------------------------------------------------------------------------------------------------------------------------|
| DESCRIPTION    | All Internet Protocol Interface Links to Signaling System 7 Signaling Gateway are Down (All IP Interface Links to SS7 Signaling Gateway are Down) |
| SEVERITY       | CRITICAL                                                                                                                                          |
| THRESHOLD      | 100                                                                                                                                               |
| THROTTLE       | 0                                                                                                                                                 |
| DATAWORDS      | Interface Name - STRING [65]<br>Interface IP Address - STRING [65]                                                                                |
| PRIMARY CAUSE  | Hardware problem has occurred.                                                                                                                    |
| PRIMARY ACTION | Check the link interfaces.                                                                                                                        |

## SIGNALING (145)

To troubleshoot and correct the cause of the alarm, refer to the [“One Internet Protocol Interface to Signaling System 7 Signaling Gateway is Down - Signaling \(145\)”](#) section on page 10-130.

|                |                                                                                                                                     |
|----------------|-------------------------------------------------------------------------------------------------------------------------------------|
| DESCRIPTION    | One Internet Protocol Interface to Signaling System 7 Signaling Gateway is Down (One IP Interface to SS7 Signaling Gateway is Down) |
| SEVERITY       | MINOR                                                                                                                               |
| THRESHOLD      | 100                                                                                                                                 |
| THROTTLE       | 0                                                                                                                                   |
| DATAWORDS      | Interface Name - STRING [65]<br>Interface IP Address - STRING [65]                                                                  |
| PRIMARY CAUSE  | Hardware problem has occurred.                                                                                                      |
| PRIMARY ACTION | Check the link interfaces.                                                                                                          |



### Note

SIGNALING (146) through SIGNALING (149) are not used.

## SIGNALING (150)

To troubleshoot and correct the cause of the alarm, refer to the [“Stream Control Transmission Protocol Association Congested - Signaling \(150\)”](#) section on page 10-130.

|                  |                                                                                         |
|------------------|-----------------------------------------------------------------------------------------|
| DESCRIPTION      | Stream Control Transmission Protocol Association Congested (SCTP Association Congested) |
| SEVERITY         | MINOR                                                                                   |
| THRESHOLD        | 100                                                                                     |
| THROTTLE         | 0                                                                                       |
| DATAWORDS        | SCTP Association ID - STRING [17]<br>Congestion Level - ONE_BYTE                        |
| PRIMARY CAUSE    | Network is congested.                                                                   |
| PRIMARY ACTION   | Clean off the network congestion caused by routing or switching issues.                 |
| SECONDARY CAUSE  | Central processing unit (CPU) is throttled.                                             |
| SECONDARY ACTION | May need upgrade to a more powerful platform or offload some traffic.                   |

# Monitoring Signaling Events

This section provides the information needed to monitor and correct Signaling events. [Table 10-2](#) lists all Signaling events in numerical order and provides cross reference to each subsection in this section.

**Table 10-2** *Cisco BTS 10200 Softswitch Signaling Events*

| Event Type    | Event Name                                                                                    | Event Severity |
|---------------|-----------------------------------------------------------------------------------------------|----------------|
| SIGNALING(1)  | <a href="#">Test Report - Signaling (1)</a>                                                   | INFO           |
| SIGNALING(2)  | <a href="#">Message Encoding Error - Signaling (2)</a>                                        | WARNING        |
| SIGNALING(3)  | <a href="#">Message Decoding Error - Signaling (3)</a>                                        | MAJOR          |
| SIGNALING(4)  | <a href="#">Invalid Message Received - Signaling (4)</a>                                      | WARNING        |
| SIGNALING(5)  | <a href="#">Database Module Function Call Failure - Signaling (6)</a>                         | N/A            |
| SIGNALING(6)  | <a href="#">Database Module Function Call Failure - Signaling (6)</a>                         | WARNING        |
| SIGNALING(7)  | <a href="#">Socket Failure - Signaling (7)</a>                                                | MAJOR          |
| SIGNALING(8)  | <a href="#">Session Initiation Protocol Message Receive Failure - Signaling (8)</a>           | MAJOR          |
| SIGNALING(9)  | <a href="#">Timeout on Internet Protocol Address - Signaling (9)</a>                          | MAJOR          |
| SIGNALING(10) | <a href="#">Failed to Send Complete Session Initiation Protocol Message - Signaling (10)</a>  | MINOR          |
| SIGNALING(11) | <a href="#">Failed to Allocate Session Initiation Protocol Control Block - Signaling (11)</a> | MAJOR          |
| SIGNALING(12) | <a href="#">Feature Server is not Up or is not Responding to Call Agent - Signaling (12)</a>  | CRITICAL       |
| SIGNALING(13) | <a href="#">Signaling System 7 Signaling Link Down - Signaling (13)</a>                       | MAJOR          |
| SIGNALING(14) | <a href="#">Link is Remotely Inhibited - Signaling (14)</a>                                   | MINOR          |
| SIGNALING(15) | <a href="#">Link is Locally Inhibited - Signaling (15)</a>                                    | MINOR          |
| SIGNALING(16) | <a href="#">Link is Congested - Signaling (16)</a>                                            | MINOR          |
| SIGNALING(17) | <a href="#">Link: Local Processor Outage - Signaling (17)</a>                                 | MINOR          |
| SIGNALING(18) | <a href="#">Link: Remote Processor Outage - Signaling (18)</a>                                | MINOR          |
| SIGNALING(19) | <a href="#">Link Set Inaccessible - Signaling (19)</a>                                        | MAJOR          |
| SIGNALING(20) | <a href="#">Link Set Congestion - Signaling (20)</a>                                          | MAJOR          |
| SIGNALING(21) | <a href="#">Route Set Failure - Signaling (21)</a>                                            | MAJOR          |
| SIGNALING(22) | <a href="#">Route Set Congested - Signaling (22)</a>                                          | MINOR          |
| SIGNALING(23) | <a href="#">Destination Point Code Unavailable - Signaling (23)</a>                           | MAJOR          |
| SIGNALING(24) | <a href="#">Destination Point Code Congested - Signaling (24)</a>                             | MINOR          |
| SIGNALING(25) | <a href="#">Unanswered Blocking Message - Signaling (25)</a>                                  | WARNING        |
| SIGNALING(26) | <a href="#">Unanswered Unblocking Message - Signaling (26)</a>                                | WARNING        |
| SIGNALING(27) | <a href="#">Unanswered Circuit Group Blocking Message - Signaling (27)</a>                    | WARNING        |
| SIGNALING(28) | <a href="#">Unanswered Circuit Group Unblocking Message - Signaling (28)</a>                  | WARNING        |
| SIGNALING(29) | <a href="#">Unanswered Circuit Query Message - Signaling (29)</a>                             | WARNING        |
| SIGNALING(30) | <a href="#">Unanswered Circuit Validation Test Message - Signaling (30)</a>                   | WARNING        |
| SIGNALING(31) | <a href="#">Unanswered Reset Circuit Message - Signaling (31)</a>                             | WARNING        |
| SIGNALING(32) | <a href="#">Unanswered Group Reset Message - Signaling (32)</a>                               | WARNING        |

**Table 10-2 Cisco BTS 10200 Softswitch Signaling Events (continued)**

| Event Type    | Event Name                                                                                                                   | Event Severity |
|---------------|------------------------------------------------------------------------------------------------------------------------------|----------------|
| SIGNALING(33) | Unanswered Release Message - Signaling (33)                                                                                  | WARNING        |
| SIGNALING(34) | Unanswered Continuity Check Request Message - Signaling (34)                                                                 | WARNING        |
| SIGNALING(35) | Trunk Locally Blocked - Signaling (36)                                                                                       | N/A            |
| SIGNALING(36) | Trunk Locally Blocked - Signaling (36)                                                                                       | MINOR          |
| SIGNALING(37) | Trunk Remotely Blocked - Signaling (40)                                                                                      | N/A            |
| SIGNALING(38) | Trunk Remotely Blocked - Signaling (40)                                                                                      | N/A            |
| SIGNALING(39) | Trunk Remotely Blocked - Signaling (40)                                                                                      | N/A            |
| SIGNALING(40) | Trunk Remotely Blocked - Signaling (40)                                                                                      | MAJOR          |
| SIGNALING(42) | Continuity Testing Message Received on the Specified Circuit Identification Code - Signaling (42)                            | INFO           |
| SIGNALING(43) | Release Complete Received in Response to Reset Circuit Message on the Specified Circuit Identification Code - Signaling (43) | INFO           |
| SIGNALING(44) | Continuity Recheck is Performed on Specified Circuit Identification Code - Signaling (44)                                    | INFO           |
| SIGNALING(45) | Circuit is UNEQUIPPED on Remote Side - Signaling (45)                                                                        | INFO           |
| SIGNALING(46) | Specified Circuit Identification Code is Invalid for the Operation - Signaling (46)                                          | INFO           |
| SIGNALING(48) | A General Processing Error Encountered - Signaling (49)                                                                      | INFO           |
| SIGNALING(49) | A General Processing Error Encountered - Signaling (49)                                                                      | INFO           |
| SIGNALING(50) | Unexpected Message for the Call State is Received: Clear Call - Signaling (50)                                               | INFO           |
| SIGNALING(51) | Set Trunk State as Remotely Unequipped - Signaling (51)                                                                      | INFO           |
| SIGNALING(52) | Set Trunk State as NOT Remotely Blocked - Signaling (52)                                                                     | INFO           |
| SIGNALING(53) | Set Trunk State as Remotely Blocked - Signaling (53)                                                                         | INFO           |
| SIGNALING(54) | Circuit Validation Test Aborted - Signaling (54)                                                                             | INFO           |
| SIGNALING(55) | Circuit Validation Successful - Signaling (55)                                                                               | INFO           |
| SIGNALING(56) | Continuity Recheck Failed - Signaling (57)                                                                                   | INFO           |
| SIGNALING(57) | Continuity Recheck Failed - Signaling (57)                                                                                   | INFO           |
| SIGNALING(58) | Continuity Recheck Successful - Signaling (58)                                                                               | INFO           |
| SIGNALING(59) | Auto State Change for Integrated Services Digital Network Trunk Group by Media Gateway - Signaling (59)                      | MAJOR          |
| SIGNALING(60) | Integrated Services Digital Network STATUS Message Containing Error Indication Received - Signaling (60)                     | WARNING        |
| SIGNALING(61) | Trunk Operational State Changed by Service Message - Signaling (61)                                                          | INFO           |
| SIGNALING(62) | Received Integrated Services Digital Network RESTART Message - Signaling (62)                                                | INFO           |
| SIGNALING(63) | Media Gateway/Termination Faulty - Signaling (63)                                                                            | MAJOR          |
| SIGNALING(64) | Media Gateway Adapter Running out of Shared Memory Pools - Signaling (64)                                                    | CRITICAL       |
| SIGNALING(65) | Media Gateway Adapter Running out of Heap Memory - Signaling (65)                                                            | CRITICAL       |
| SIGNALING(66) | Call Agent Internal Error (Because of Which Media Gateway Adapter has to Start Automatically) - Signaling (66)               | MAJOR          |

**Table 10-2 Cisco BTS 10200 Softswitch Signaling Events (continued)**

| Event Type    | Event Name                                                                                                        | Event Severity |
|---------------|-------------------------------------------------------------------------------------------------------------------|----------------|
| SIGNALING(68) | Media Gateway or Termination are Found Administratively Out of Service - Signaling (68)                           | MAJOR          |
| SIGNALING(69) | Call Agent and Feature Server Communication Message Timeout - Signaling (69)                                      | CRITICAL       |
| SIGNALING(70) | Integrated Services Digital Network Unable to Restore D-channel Due to Failed Communication - Signaling (70)      | WARNING        |
| SIGNALING(71) | Integrated Services Digital Network Unable to Establish D-channel - Signaling (71)                                | WARNING        |
| SIGNALING(72) | Integrated Services Digital Network - Calls Lost Due to D-channel Down for Period of Time - Signaling (72)        | WARNING        |
| SIGNALING(73) | Integrated Services Digital Network - Unable to Send RESTART Due to RESTART Timer Expired - Signaling (73)        | WARNING        |
| SIGNALING(74) | Integrated Services Digital Network: Unable to Send the SERVICE Due to the SERVICE Timer Expired - Signaling (74) | WARNING        |
| SIGNALING(75) | Signaling System 7 Stack not Ready - Signaling (75)                                                               | CRITICAL       |
| SIGNALING(76) | Timeout on Remote Instance - Signaling (76)                                                                       | INFO           |
| SIGNALING(77) | Integrated Services Digital Network D-channel Switchover for Non-Facility Associated Signaling - Signaling (77)   | INFO           |
| SIGNALING(78) | Integrated Services Digital Network Single D-channel Down for Non-Facility Associated Signaling - Signaling (78)  | MINOR          |
| SIGNALING(79) | Media Gateway Unreachable - Signaling (79)                                                                        | MAJOR          |
| SIGNALING(80) | Out of Bounds, Memory/Socket Error - Signaling (80)                                                               | CRITICAL       |
| SIGNALING(81) | Insufficient Heap Memory - Signaling (81) (H.323)                                                                 | CRITICAL       |
| SIGNALING(82) | Insufficient Shared Memory Pools - Signaling (82) (H.323)                                                         | CRITICAL       |
| SIGNALING(83) | Error While Binding to Socket - Signaling (83)                                                                    | CRITICAL       |
| SIGNALING(84) | Reached Maximum Socket Limit - Signaling (84) (H.323)                                                             | CRITICAL       |
| SIGNALING(85) | Initialization Failure - Signaling (85)                                                                           | CRITICAL       |
| SIGNALING(86) | Remote H323 Gateway is not Reachable - Signaling (86) (H.323)                                                     | MAJOR          |
| SIGNALING(87) | H323 Message Parsing Error - Signaling (87) (H.323)                                                               | MAJOR          |
| SIGNALING(88) | H323 Message Encoding Error - Signaling (88) (H.323)                                                              | MAJOR          |
| SIGNALING(89) | Gatekeeper not Available/Reachable - Signaling (89)                                                               | MAJOR          |
| SIGNALING(90) | Alternate Gatekeeper is not Responding - Signaling (90)                                                           | MAJOR          |
| SIGNALING(91) | Endpoint Security Violation - Signaling (91) (H.323)                                                              | MAJOR          |
| SIGNALING(92) | Invalid Call Identifier - Signaling (92)                                                                          | MINOR          |
| SIGNALING(93) | Invalid Call Reference Value - Signaling (93)                                                                     | MINOR          |
| SIGNALING(94) | Invalid Conference Identifier - Signaling (94)                                                                    | MINOR          |
| SIGNALING(95) | Invalid Message from the Network - Signaling (95)                                                                 | MINOR          |
| SIGNALING(96) | Internal Call Processing Error - Signaling (96)                                                                   | MINOR          |
| SIGNALING(97) | Insufficient Information to Complete Call - Signaling (97)                                                        | MINOR          |
| SIGNALING(98) | H323 Protocol Inconsistencies - Signaling (98) (H.323)                                                            | MINOR          |

**Table 10-2 Cisco BTS 10200 Softswitch Signaling Events (continued)**

| Event Type     | Event Name                                                                                                                  | Event Severity |
|----------------|-----------------------------------------------------------------------------------------------------------------------------|----------------|
| SIGNALING(99)  | Abnormal Call Clearing - Signaling (99)                                                                                     | MINOR          |
| SIGNALING(100) | Codec Negotiation Failed - Signaling (100)                                                                                  | MINOR          |
| SIGNALING(101) | Per Call Security Violation - Signaling (101)                                                                               | MINOR          |
| SIGNALING(102) | H323 Network Congested - Signaling (102) (H.323)                                                                            | MINOR          |
| SIGNALING(103) | Aggregation Connection Down - Signaling (103)                                                                               | MAJOR          |
| SIGNALING(104) | Aggregation Unable To Establish Connection - Signaling (104)                                                                | INFO           |
| SIGNALING(105) | Aggregation Gate Set Failed - Signaling (105)                                                                               | INFO           |
| SIGNALING(106) | Enhanced Subscriber Authentication Cisco BTS 10200 Softswitch Delivery Function Connection Down - Signaling (106)           | MINOR          |
| SIGNALING(107) | Logical Internet Protocol Addresses not Mapped Correctly - Signaling (107)                                                  | CRITICAL       |
| SIGNALING(108) | Current SIA Configuration only Valid for Simplex Systems - Signaling (108)                                                  | MAJOR          |
| SIGNALING(109) | Stream Control Transmission Protocol Association Failure - Signaling (109)                                                  | MAJOR          |
| SIGNALING(110) | Signaling Gateway Group is Out-of-Service - Signaling (110)                                                                 | CRITICAL       |
| SIGNALING(111) | Stream Control Transmission Protocol Association Degraded (One of Two Internet Protocol Connections Down) - Signaling (111) | MAJOR          |
| SIGNALING(112) | Stream Control Transmission Protocol Association Configuration Error - Signaling (112)                                      | MINOR          |
| SIGNALING(113) | Signaling Gateway Failure - Signaling (113)                                                                                 | MAJOR          |
| SIGNALING(114) | Signaling Gateway Process is Out-of-Service - Signaling (114)                                                               | MAJOR          |
| SIGNALING(115) | Invalid Routing Context Received - Signaling (115)                                                                          | WARNING        |
| SIGNALING(116) | Destination Point Code User Part Unavailable - Signaling (116)                                                              | MAJOR          |
| SIGNALING(117) | Circuit Validation Test Message Received for an Unequipped Circuit Identification Code - Signaling (117)                    | MINOR          |
| SIGNALING(118) | Circuit Verification Response Received with Failed Indication - Signaling (118)                                             | MINOR          |
| SIGNALING(119) | Signaling System 7 Adapter Process Faulty - Signaling (119)                                                                 | CRITICAL       |
| SIGNALING(120) | Signaling System 7 Module/Signaling System 7 Adapter Faulty - Signaling (120)                                               | CRITICAL       |
| SIGNALING(121) | Message Transfer Part 3 User Adapter Cannot Go Standby - Signaling (121)                                                    | MAJOR          |
| SIGNALING(122) | Message Transfer Part 3 User Adapter Cannot Go Active - Signaling (122)                                                     | MAJOR          |
| SIGNALING(123) | Remote Subsystem is out of Service - Signaling (124)                                                                        | MINOR          |
| SIGNALING(124) | Remote Subsystem is out of Service - Signaling (124)                                                                        | MINOR          |
| SIGNALING(125) | Signaling Connection Control Part Routing Error - Signaling (125)                                                           | MAJOR          |
| SIGNALING(126) | Signaling Connection Control Binding Failure - Signaling (126)                                                              | MAJOR          |
| SIGNALING(127) | Transaction Capabilities Application Part Binding Failure - Signaling (127)                                                 | MAJOR          |
| SIGNALING(129) | Transaction Capabilities Application Part Reaches the Provisioned Resource Limit - Signaling (132)                          | N/A            |
| SIGNALING(130) | Transaction Capabilities Application Part Reaches the Provisioned Resource Limit - Signaling (132)                          | N/A            |



**Table 10-2** Cisco BTS 10200 Softswitch Signaling Events (continued)

| Event Type     | Event Name                                                                                             | Event Severity |
|----------------|--------------------------------------------------------------------------------------------------------|----------------|
| SIGNALING(131) | Transaction Capabilities Application Part Reaches the Provisioned Resource Limit - Signaling (132)     | WARNING        |
| SIGNALING(132) | Transaction Capabilities Application Part Reaches the Provisioned Resource Limit - Signaling (132)     | WARNING        |
| SIGNALING(133) | Unable to Decode Generic Transport Descriptor Message - Signaling (133)                                | INFO           |
| SIGNALING(134) | Signaling System 7 Message Encoding Failure - Signaling (134)                                          | INFO           |
| SIGNALING(135) | Signaling System 7 Message Decoding Failure - Signaling (135)                                          | INFO           |
| SIGNALING(136) | Signaling System 7 Message Invalid Received - Signaling (136)                                          | INFO           |
| SIGNALING(137) | Signaling System 7 Confusion Message Received - Signaling (137)                                        | INFO           |
| SIGNALING(138) | Number of Open Session Initiation Protocol Connections is Reaching Engineered Limit - Signaling (138)  | WARNING        |
| SIGNALING(139) | Signaling System 7 Trunk was Found to be in Erroneous State - Signaling (139) (SS7)                    | INFO           |
| SIGNALING(140) | Unanswered Information Message - Signaling (140)                                                       | INFO           |
| SIGNALING(141) | Address not Resolved by Domain Name System Server - Signaling (141)                                    | WARNING        |
| SIGNALING(142) | Session Initiation Protocol Trunk Operationally Out-of-Service - Signaling (142)                       | CRITICAL       |
| SIGNALING(143) | Internet Protocol Interface Link to the Signaling System 7 Signaling Gateway is Down - Signaling (143) | MINOR          |
| SIGNALING(144) | All Internet Interface Links to Signaling System 7 Signaling Gateway are Down - Signaling (144)        | CRITICAL       |
| SIGNALING(145) | One Internet Protocol Interface to Signaling System 7 Signaling Gateway is Down - Signaling (145)      | MINOR          |
| SIGNALING(146) | Stream Control Transmission Protocol Association Congested - Signaling (150)                           | WARNING        |
| SIGNALING(147) | Stream Control Transmission Protocol Association Congested - Signaling (150)                           | WARNING        |
| SIGNALING(148) | Stream Control Transmission Protocol Association Congested - Signaling (150)                           | WARNING        |
| SIGNALING(149) | Stream Control Transmission Protocol Association Congested - Signaling (150)                           | MAJOR          |
| SIGNALING(150) | Stream Control Transmission Protocol Association Congested - Signaling (150)                           | MINOR          |
| SIGNALING(151) | Troubleshooting Signaling Alarms                                                                       | MINOR          |

## Test Report - Signaling (1)

The Test Report event is for testing the signaling event category. The event is informational and no further action is required.

## Message Encoding Error - Signaling (2)

The Message Encoding Error event serves as a warning that a message encoding error has occurred. The event is issued when there is a message encoding error on sending an MGCP message. If the event is issued while doing interoperability testing with a gateway using MGCP, then capture the MGCP message flow and forward it to Cisco TAC technical support for analysis. When an unexpected MGCP message occurs, contact Cisco TAC technical support to identify the root cause. Refer to the [“Obtaining Technical Assistance” section on page xxxviii](#) for detailed instructions on contacting Cisco TAC and opening a service request.

## Message Decoding Error - Signaling (3)

The Message Decoding Error event serves as a warning that a message decoding error has occurred. The event is issued when there is a message decoding error on receiving an MGCP message. If this event is issued while doing interoperability testing with a gateway using MGCP, then capture the MGCP message flow and forward it to Cisco TAC technical support for analysis. When an unexpected MGCP message occurs, call Cisco TAC technical support to identify the root cause. Refer to the [“Obtaining Technical Assistance” section on page xxxviii](#) for detailed instructions on contacting Cisco TAC and opening a service request.

## Invalid Message Received - Signaling (4)

The Invalid Message Received event serves as a warning that an invalid message has been received. The primary cause of the event is that a signaling adapter has received an invalid message from the specified endpoint. To correct the primary cause of the event, monitor the associated signaling link to see if there is an interruption of service on the link. If there is a communication problem, restart the link. Verify that the version of the protocol used by the device at the endpoint is consistent with the version expected by the call agent. If there is a mismatch, then either the endpoint or call agent must be re-provisioned.

## Database Module Function Call Failure - Signaling (6)

The Database Module Function Call Failure event serves as a warning that a database module function call has failed. The primary cause of the event is that a signaling adapter has detected an error while accessing a database interface. To correct the primary cause of the event, restart the associated process if the database that the adapter attempted to access is not available. If incompatible versions of the signaling adapter process and the database processes are present on the system, correct the error and restart the processes.

## Socket Failure - Signaling (7)

The Socket Failure alarm (major) indicates that there is a failure in creating the UDP port used by the MGCP stacks. To troubleshoot and correct the cause of the Socket Failure alarm, refer to the [“Socket Failure - Signaling \(7\)” section on page 10-106](#).

## Session Initiation Protocol Message Receive Failure - Signaling (8)

The Session Initiation Protocol Message Receive Failure alarm (major) indicates that a SIP message receive has failed. To troubleshoot and correct the cause of the Session Initiation Protocol Message Receive Failure alarm, refer to the [“Session Initiation Protocol Message Receive Failure - Signaling \(8\)” section on page 10-106](#).

## Timeout on Internet Protocol Address - Signaling (9)

The Timeout on Internet Protocol Address alarm (major) indicates that an IP address has timed out. To troubleshoot and correct the cause of the Timeout on Internet Protocol Address alarm, refer to the [“Timeout on Internet Protocol Address - Signaling \(9\)” section on page 10-107](#).

## Failed to Send Complete Session Initiation Protocol Message - Signaling (10)

The Failed to Send Complete Session Initiation Protocol Message alarm (minor) indicates that a SIP message failure has occurred. To troubleshoot and correct the cause of the Failed to Send Complete Session Initiation Protocol Message alarm, refer to the [“Failed to Send Complete Session Initiation Protocol Message - Signaling \(10\)” section on page 10-107](#).

## Failed to Allocate Session Initiation Protocol Control Block - Signaling (11)

The Failed to Allocate Session Initiation Protocol Control Block alarm (major) indicates that a SIP control block allocation failed. To troubleshoot and correct the cause of the Failed to Allocate Session Initiation Protocol Control Block alarm, refer to the [“Failed to Allocate Session Initiation Protocol Control Block - Signaling \(11\)” section on page 10-107](#).

## Feature Server is not Up or is not Responding to Call Agent - Signaling (12)

The Feature Server is not Up or is not Responding to Call Agent alarm (critical) indicates that the feature server is not up or is not responding to the call agent server. To troubleshoot and correct the cause of the Feature Server is not Up or is not Responding to Call Agent alarm, refer to the [“Feature Server is not Up or is not Responding to Call Agent - Signaling \(12\)” section on page 10-108](#).

## Signaling System 7 Signaling Link Down - Signaling (13)

The Signaling System 7 Signaling Link Down alarm (major) indicates the SS7 signaling link is down. To troubleshoot and correct the cause of the Signaling System 7 Signaling Link Down alarm, refer to the [“Signaling System 7 Signaling Link Down - Signaling \(13\)” section on page 10-108](#).

## Link is Remotely Inhibited - Signaling (14)

The Link is Remotely Inhibited alarm (minor) indicates that the SS7 link is inhibited at the remote end. To troubleshoot and correct the cause of the Link is Remotely Inhibited alarm, refer to the [“Link is Remotely Inhibited - Signaling \(14\)” section on page 10-108](#).

## Link is Locally Inhibited - Signaling (15)

The Link is Locally Inhibited alarm (minor) indicates that the SS7 link is inhibited at the local end. To troubleshoot and correct the cause of the Link is Locally Inhibited alarm, refer to the [“Link is Locally Inhibited - Signaling \(15\)” section on page 10-108](#).

## Link is Congested - Signaling (16)

The Link is Congested alarm (minor) indicates that the SS7 link is congested. To troubleshoot and correct the cause of the Link is Congested alarm, refer to the [“Link is Congested - Signaling \(16\)” section on page 10-109](#).

## Link: Local Processor Outage - Signaling (17)

The Link: Local Processor Outage alarm (minor) indicates that the SS7 link has experienced a local processor outage. To troubleshoot and correct the cause of the Link: Local Processor Outage alarm, refer to the [“Link: Local Processor Outage - Signaling \(17\)” section on page 10-109](#).

## Link: Remote Processor Outage - Signaling (18)

The Link: Remote Processor Outage alarm (minor) indicates that the SS7 link has experienced a remote processor outage. To troubleshoot and correct the cause of the Link: Remote Processor Outage alarm, refer to the [“Link: Remote Processor Outage - Signaling \(18\)” section on page 10-109](#).

## Link Set Inaccessible - Signaling (19)

The Link Set Inaccessible alarm (major) indicates that the specified SS7 link is inaccessible. To troubleshoot and correct the cause of the Link Set Inaccessible alarm, refer to the [“Link Set Inaccessible - Signaling \(19\)” section on page 10-109](#).

## Link Set Congestion - Signaling (20)

The Link Set Congestion alarm (major) indicates that the specified SS7 link set is congested. To troubleshoot and correct the cause of the Link Set Congestion alarm, refer to the [“Link Set Congestion - Signaling \(20\)” section on page 10-109](#).

## Route Set Failure - Signaling (21)

The Route Set Failure alarm (major) indicates that the specified route set has experienced a failure. To troubleshoot and correct the cause of the Route Set Failure alarm, refer to the [“Route Set Failure - Signaling \(21\)” section on page 10-110](#).

## Route Set Congested - Signaling (22)

The Route Set Congested alarm (minor) indicates that the specified route set is congested. To troubleshoot and correct the cause of the Route Set Congested alarm, refer to the [“Route Set Congested - Signaling \(22\)” section on page 10-110](#).

## Destination Point Code Unavailable - Signaling (23)

The Destination Point Code Unavailable alarm (major) indicates that the specified DPC is not available. To troubleshoot and correct the cause of the Destination Point Code Unavailable alarm, refer to the [“Destination Point Code Unavailable - Signaling \(23\)” section on page 10-111](#).

## Destination Point Code Congested - Signaling (24)

The Destination Point Code Congested alarm (minor) alarm indicates that the specified DPC is congested. To troubleshoot and correct the cause of the Destination Point Code Congested alarm, refer to the [“Destination Point Code Congested - Signaling \(24\)” section on page 10-112](#).

## Unanswered Blocking Message - Signaling (25)

The Unanswered Blocking Message event serves as a warning that a BLO message was not answered. The primary cause of the event is that a BLO message was not acknowledged before the T13 expired for the associated CIC. To correct the primary cause of the event, verify that the SS7 signaling adapter processes is running normally. Verify that the call agent platform is active. Verify that the SS7 interface hardware is in service. Verify that the associated SS7 signaling link is available. Verify that the T13 timer is set to an appropriate level. Verify that the SS7 link is not congested.

## Unanswered Unblocking Message - Signaling (26)

The Unanswered Unblocking Message event serves as a warning that an UBL message was not answered. The primary cause of the event is that a UBL message was not acknowledged before the T15 expired for the associated CIC. To correct the primary cause of the event, verify that the SS7 signaling adapter processes is running normally. Verify that the call agent platform is active. Verify that the SS7 interface hardware is in service. Verify that the associated SS7 signaling link is available. Verify that the T13 timer is set to an appropriate level. Verify that the SS7 link is not congested.

## Unanswered Circuit Group Blocking Message - Signaling (27)

The Unanswered Circuit Group Blocking Message event serves as a warning that a CGB message was not answered. The primary cause of the event is that a CGB message was not acknowledged before the T19 expired for the associated CIC. To correct the primary cause of the event, verify that the SS7 signaling adapter processes is running normally. Verify that the call agent platform is active. Verify that the SS7 interface hardware is in service. Verify that the associated SS7 signaling link is available. Verify that the T13 timer is set to an appropriate level. Verify that the SS7 link is not congested.

## Unanswered Circuit Group Unblocking Message - Signaling (28)

The Unanswered Circuit Group Unblocking Message event serves as a warning that a CGU message was not answered. The primary cause of the event is that a CGU message was not acknowledged before the T21 expired for the associated CIC. To correct the primary cause of the event, verify that the SS7 signaling adapter processes is running normally. Verify that the call agent platform is active. Verify that the SS7 interface hardware is in service. Verify that the associated SS7 signaling link is available. Verify that the T13 timer is set to an appropriate level. Verify that the SS7 link is not congested.

## Unanswered Circuit Query Message - Signaling (29)

The Unanswered Circuit Query Message event serves as a warning that a CQM message was not answered. The primary cause of the event is that a CQM message was not acknowledged before the T28 expired for the associated CIC. To correct the primary cause of the event, verify that the SS7 signaling adapter processes is running normally. Verify that the call agent platform is active. Verify that the SS7 interface hardware is in service. Verify that the associated SS7 signaling link is available. Verify that the T13 timer is set to an appropriate level. Verify that the SS7 link is not congested.

## Unanswered Circuit Validation Test Message - Signaling (30)

The Unanswered Circuit Validation Test Message event serves as a warning that a CVT message was not answered. The primary cause of the event is that a CVT message was not acknowledged before the Tcvr expired for the associated CIC. To correct the primary cause of the event, verify that the SS7 signaling adapter processes is running normally. Verify that the call agent platform is active. Verify that the SS7 interface hardware is in service. Verify that the associated SS7 signaling link is available. Verify that the T13 timer is set to an appropriate level. Verify that the SS7 link is not congested.

## Unanswered Reset Circuit Message - Signaling (31)

The Unanswered Reset Circuit Message event serves as a warning that a RSC message was not answered. The primary cause of the event is that a RSC message was not acknowledged before the T17 expired for the associated CIC. To correct the primary cause of the event, verify that the SS7 signaling adapter processes is running normally. Verify that the call agent platform is active. Verify that the SS7 interface hardware is in service. Verify that the associated SS7 signaling link is available. Verify that the T13 timer is set to an appropriate level. Verify that the SS7 link is not congested.

## Unanswered Group Reset Message - Signaling (32)

The Unanswered Group Reset Message event serves as a warning that a GRS message was not answered. The primary cause of the event is that a GRS message was not acknowledged before the T23 expired for the associated CIC. To correct the primary cause of the event, verify that the SS7 signaling adapter processes is running normally. verify that the call agent platform is active. Verify that the SS7 interface hardware is in service. Verify that the associated SS7 signaling link is available. Verify that the T13 timer is set to an appropriate level. Verify that the SS7 link is not congested.

## Unanswered Release Message - Signaling (33)

The Unanswered Release Message event serves as a warning that a REL message was not answered. The primary cause of the event is that a REL message was not acknowledged before the T5 expired for the associated CIC. To correct the primary cause of the event, verify that the SS7 signaling adapter processes is running normally. Verify that the call agent platform is active. Verify that the SS7 interface hardware is in service. Verify that the associated SS7 signaling link is available. Verify that the T13 timer is set to an appropriate level. Verify that the SS7 link is not congested.

## Unanswered Continuity Check Request Message - Signaling (34)

The Unanswered Continuity Check Request Message event serves as a warning that a continuity check request (CCR) message was not answered. The primary cause of the event is that a LPA message was not acknowledged before the T<sub>CCR</sub> expired for the associated CIC. To correct the primary cause of the event, verify that the SS7 signaling adapter processes is running normally. Verify that the call agent platform is active. Verify that the SS7 interface hardware is in service. Verify that the associated SS7 signaling link is available. Verify that the T13 timer is set to an appropriate level. Verify that the SS7 link is not congested.

## Trunk Locally Blocked - Signaling (36)

The Trunk Locally Blocked alarm (minor) indicates that the trunk is locally blocked. To troubleshoot and correct the cause of the Trunk Locally Blocked alarm, refer to the [“Trunk Locally Blocked - Signaling \(36\)” section on page 10-112](#). For additional troubleshooting information, refer to Appendix A, “System Usage of MGW Keepalive Parameters, Release 4.4.x.”

## Trunk Remotely Blocked - Signaling (40)

The Trunk Remotely Blocked alarm (major) indicates that the trunk is remotely blocked. To troubleshoot and correct the cause of the Trunk Remotely Blocked alarm, refer to the [“Trunk Remotely Blocked - Signaling \(40\)” section on page 10-112](#).

## Continuity Testing Message Received on the Specified Circuit Identification Code - Signaling (42)

The Continuity Testing Message Received on the Specified Circuit Identification Code event functions as an informational alert that the COT message was received on the specified CIC. The event is informational and no further action is required.

## **Release Complete Received in Response to Reset Circuit Message on the Specified Circuit Identification Code - Signaling (43)**

The Release Complete Received in Response to Reset Circuit Message on the Specified Circuit Identification Code event functions as an informational alert that the RLC was received in response to the RSC message received on the specified CIC. The event is informational and no further action is required.

## **Continuity Recheck is Performed on Specified Circuit Identification Code - Signaling (44)**

The Continuity Recheck is Performed on Specified Circuit Identification Code event functions as an informational alert that a continuity recheck was performed on the specified CIC. The event is informational and further action is required.

## **Circuit is UNEQUIPPED on Remote Side - Signaling (45)**

The Circuit is UNEQUIPPED on Remote Side event functions as an informational alert the circuit is unequipped on the remote side. The primary cause of the event is that an unequipped circuit has been detected on the remote side. To correct the primary cause of the event, monitor the event reports at the network level to verify if an existing circuit was unequipped causing a status mismatch with the local end.

## **Specified Circuit Identification Code is Invalid for the Operation - Signaling (46)**

The Specified Circuit Identification Code is Invalid for the Operation event functions as an informational alert that the specified CIC is invalid for the attempted operation. The primary cause of the event is that an invalid operation was performed on the specified CIC. To correct the primary cause of the event, verify that the SS7 provisioning tables are properly configured at the circuit level.

## **A General Processing Error Encountered - Signaling (49)**

The A General Processing Error Encountered event functions as an informational alert that a general processing error has occurred. The primary cause of the event is that a general SS7 processing error occurred due to all resources being busy or an invalid event occurring. To correct the primary cause of the event, verify the status of the signaling adapter process and the SS7 signaling interface to verify proper operation.

## **Unexpected Message for the Call State is Received: Clear Call - Signaling (50)**

The Unexpected Message for the Call State is Received: Clear Call event functions as an informational alert that an unexpected message for the call state has been received. The primary cause of the event is that an unexpected message was received for the current call state. To correct the primary cause of the event, verify the status of the signaling adapter process and the SS7 signaling interface to verify proper operation.



## Set Trunk State as Remotely Unequipped - Signaling (51)

The Set Trunk State as Remotely Unequipped event functions as an informational alert that the trunk state is currently set as remotely unequipped. The primary cause of the event is that the specified CIC is marked as remotely unequipped due to the CQM response indicating that it is unequipped at the far end. To correct the primary cause of the event, equip the trunk circuit at the far end.

## Set Trunk State as NOT Remotely Blocked - Signaling (52)

The Set Trunk State as NOT Remotely Blocked event functions as an informational alert that the trunk state has been set as not remotely blocked. The primary cause of the event is that the specified CIC is marked as not remotely blocked due to the CQM response indicating that it is not remotely blocked at the far end. The event is informational and no further action is required.

## Set Trunk State as Remotely Blocked - Signaling (53)

The Set Trunk State as Remotely Blocked event functions as an informational alert that the trunk state is set as remotely blocked. The primary cause of the event is that the specified CIC is marked as remotely blocked due to the CQM response indicating that it is remotely blocked at the far end. To correct the primary cause of the event, clear the blocking situation at the far end based on network level event reports.

## Circuit Validation Test Aborted - Signaling (54)

The Circuit Validation Test Aborted event functions as an informational alert that the circuit validation test has been aborted. The primary cause of the event is that the circuit specified failed a validation test due to an internal failure. To correct the primary cause of the event, verify the SS7 signaling adapter process and SS7 interface is operating normally.

## Circuit Validation Successful - Signaling (55)

The Circuit Validation Successful event functions as an informational alert that the circuit validation was successful. The event is informational and no further actions is required.

## Continuity Recheck Failed - Signaling (57)

The Continuity Recheck Failed event functions as an informational alert that the continuity recheck failed. The primary cause of the event is that a continuity recheck of the specified CIC failed. To correct the primary cause of the event, verify the SS7 signaling adapter process and SS7 interface is operating normally.

## Continuity Recheck Successful - Signaling (58)

The Continuity Recheck Successful event functions as an informational alert that the continuity recheck of the specified CIC was successful. The event is informational and no further action is required.

## Auto State Change for Integrated Services Digital Network Trunk Group by Media Gateway - Signaling (59)

The Auto State Change for Integrated Services Digital Network Trunk Group by Media Gateway alarm (major) indicates that specified ISDN trunk group status was changed due to a media gateway operation. To troubleshoot and correct the cause of the Auto State Change for Integrated Services Digital Network Trunk Group by Media Gateway alarm, refer to the [“Auto State Change for Integrated Services Digital Network Trunk Group by Media Gateway - Signaling \(59\)”](#) section on page 10-112.

## Integrated Services Digital Network STATUS Message Containing Error Indication Received - Signaling (60)

The Integrated Services Digital Network STATUS Message Containing Error Indication Received event functions as a warning that an ISDN status message containing an error indication has been received. The primary cause of the event is that an ISDN status message was received containing an error indication for the specified termination. To correct the primary cause of the event, place the specified termination in service state if the specified termination is not operating normally.

## Trunk Operational State Changed by Service Message - Signaling (61)

The Trunk Operational State Changed by Service Message event functions as an informational alert that the trunk operational state was changed by a service message. The primary cause of the event is that the specified trunk group operational status was changed via a service message from the specified gateway. To correct the primary cause of the event, monitor the event reports at the network level to verify that the specified gateway and terminations are operating normally.

## Received Integrated Services Digital Network RESTART Message - Signaling (62)

The Received Integrated Services Digital Network RESTART Message event functions as an informational alert that a ISDN restart message was received. The primary cause of the event is that an ISDN restart message was received from the specified gateway. To correct the primary cause of the event, monitor the event reports at the network level to verify that the specified gateway and terminations are operating normally.

## Media Gateway/Termination Faulty - Signaling (63)

The Media Gateway/Termination Faulty alarm (major) indicates that a media gateway or termination has gone faulty due to the detection of an unknown endpoint, unknown package type, and unknown event, a hardware failure, or a general call agent error. To troubleshoot and correct the cause of the Media Gateway/Termination Faulty alarm, refer to the [“Media Gateway/Termination Faulty - Signaling \(63\)”](#) section on page 10-113.

## Media Gateway Adapter Running out of Shared Memory Pools - Signaling (64)

The Media Gateway Adapter Running out of Shared Memory Pools alarm (critical) indicates that the MGCP signaling adapter was unable to allocate data store for an IPC message due to a lack of resources. To troubleshoot and correct the cause of the Media Gateway Adapter Running out of Shared Memory Pools alarm, refer to the [“Media Gateway Adapter Running out of Shared Memory Pools - Signaling \(64\)” section on page 10-113.](#)

## Media Gateway Adapter Running out of Heap Memory - Signaling (65)

The Media Gateway Adapter Running out of Heap Memory alarm (critical) indicates that the MGCP signaling adapter was unable to allocate data store for an IPC message from the heap due to a lack of resources. To troubleshoot and correct the cause of the Media Gateway Adapter Running out of Heap Memory alarm, refer to the [“Media Gateway Adapter Running out of Heap Memory - Signaling \(65\)” section on page 10-113.](#)

## Call Agent Internal Error (Because of Which Media Gateway Adapter has to Start Automatically) - Signaling (66)

The Call Agent Internal Error (Because of Which Media Gateway Adapter has to Start Automatically) alarm (major) indicates that a call agent internal error has occurred causing the restart of the MGCP signaling adapter. To troubleshoot and correct the cause of the Call Agent Internal Error (Because of Which Media Gateway Adapter has to Start Automatically) alarm, refer to the [“Call Agent Internal Error \(Because of Which Media Gateway Adapter has to Start Automatically\) - Signaling \(66\)” section on page 10-113.](#)

## Media Gateway or Termination are Found Administratively Out of Service - Signaling (68)

The Media Gateway or Termination are Found Administratively Out of Service alarm (major) indicates that the specified media gateway is going out-of-service due to being powered down, the MGCP application going faulty, or a hardware failure has occurred. To troubleshoot and correct the cause of the Media Gateway or Termination are Found Administratively Out of Service alarm, refer to the [“Media Gateway or Termination are Found Administratively Out of Service - Signaling \(68\)” section on page 10-114.](#) For additional troubleshooting information, refer to [Appendix A, “System Usage of MGW Keepalive Parameters, Release 4.4.x.”](#)

## Call Agent and Feature Server Communication Message Timeout - Signaling (69)

The Call Agent and Feature Server Communication Message Timeout alarm (critical) indicates that a CA and FS communications message timed out. To troubleshoot correct the cause of the Call Agent and Feature Server Communication Message Timeout alarm, refer to the [“Call Agent and Feature Server Communication Message Timeout - Signaling \(69\)” section on page 10-114.](#)

## **Integrated Services Digital Network Unable to Restore D-channel Due to Failed Communication - Signaling (70)**

The Integrated Services Digital Network Unable to Restore D-channel Due to Failed Communication event serves as a warning that the ISDN signaling adapter is unable to restore D-channel due to a communication failure. The primary cause of the event is that the ISDN signaling adapter is unable to restore a D-channel due to incorrect backhaul provisioning at the media gateway or call agent. To correct the primary cause of the event, ensure the provisioning of the backhaul port is correct at both the call agent and media gateway.

## **Integrated Services Digital Network Unable to Establish D-channel - Signaling (71)**

The Integrated Services Digital Network Unable to Establish D-channel event serves as a warning that the ISDN signaling adaptor is unable to establish D-channel. The primary cause of the event is that ISDN signaling adapter is unable to establish a D-channel due to layer 1 parameters not being provisioned correctly or improper provisioning of the network or user side. To correct the primary cause of the event, verify the correct provisioning at the media gateway.

## **Integrated Services Digital Network - Calls Lost Due to D-channel Down for Period of Time - Signaling (72)**

The Integrated Services Digital Network - Calls Lost Due to D-channel Down for Period of Time event serves as a warning that calls were lost due to the D-channels being down for a period of time. The primary cause of the event is that ISDN signaling adapter has lost calls due to a D-channel being down as a result of a media gateway power loss or a loss of connection between the PBX and media gateway. To correct the primary cause of the event, resupply power to the media gateway and verify that the connection between the PBX and media gateway is intact.

## **Integrated Services Digital Network - Unable to Send RESTART Due to RESTART Timer Expired - Signaling (73)**

The Integrated Services Digital Network - Unable to Send RESTART Due to RESTART Timer Expired event serves as a warning that the ISDN signaling adapter was unable to send a restart due to the restart timer being expired. The primary cause of the event is that the ISDN signaling adapter was unable to send a RESTART message due to the expiration of the RESTART timer. To correct the primary cause of the event, verify that the RESTART timer is set to an appropriate level.

## Integrated Services Digital Network: Unable to Send the SERVICE Due to the SERVICE Timer Expired - Signaling (74)

The Integrated Services Digital Network: Unable to Send the SERVICE Due to the SERVICE Timer Expired event serves as a warning that the ISDN signal adapter was unable to send a service message due to the service timer being expired. The primary cause of the event is that the ISDN signaling adapter was unable to send a SERVICE message due to the expiration of the SERVICE timer. To correct the primary cause of the event, ensure that the RESTART timer is set to an appropriate level.

## Signaling System 7 Stack not Ready - Signaling (75)

The Signaling System 7 Stack not Ready alarm (critical) indicates that the SS7 stack is not ready. To trouble and correct the cause of the Signaling System 7 Stack not Ready alarm, refer to the [“Signaling System 7 Stack not Ready - Signaling \(75\)”](#) section on page 10-114.

## Timeout on Remote Instance - Signaling (76)

The Timeout on Remote Instance event functions as an informational alert that communication on a remote instance timed out. The primary cause of the event is that communication between call agent and remote instance is faulty. The event is informational and no further action is required.

## Integrated Services Digital Network D-channel Switchover for Non-Facility Associated Signaling - Signaling (77)

The Integrated Services Digital Network D-channel Switchover for Non-Facility Associated Signaling event functions as an informational alert that an ISDN D-channel switchover has occurred non-facility associated signaling (NFAS). The primary cause of the event is that the operator manually switched the D-channels using the CLI. To verify the primary cause of the event, verify operator action. The secondary cause of the event is that the active D-channel was lost. To correct the secondary cause of the event, verify that gateway is operational and connection to PBX is good.

## Integrated Services Digital Network Single D-channel Down for Non-Facility Associated Signaling - Signaling (78)

The Integrated Services Digital Network Single D-channel Down for Non-Facility Associated Signaling alarm (minor) indicates that one of the ISDN D-channels in the PRI is down. To troubleshoot and correct the cause of the Integrated Services Digital Network Single D-channel Down for Non-Facility Associated Signaling alarm, refer to the [“Integrated Services Digital Network Single D-channel Down for Non-Facility Associated Signaling - Signaling \(78\)”](#) section on page 10-114.

## Media Gateway Unreachable - Signaling (79)

The Media Gateway Unreachable alarm (major) indicates that the media gateway is unreachable. To troubleshoot and correct the cause of the Media Gateway Unreachable alarm, refer to the [“Media Gateway Unreachable - Signaling \(79\)” section on page 10-114](#). For additional troubleshooting information, refer to [Appendix A, “System Usage of MGW Keepalive Parameters, Release 4.4.x.”](#)

## Out of Bounds, Memory/Socket Error - Signaling (80)

The Out of Bounds, Memory/Socket Error alarm (critical) indicates that a memory socket out of bounds error has occurred. To troubleshoot and correct the cause of the Out of Bounds, Memory/Socket Error alarm, refer to the [“Out of Bounds, Memory/Socket Error - Signaling \(80\)” section on page 10-115](#).

## Insufficient Heap Memory - Signaling (81) (H.323)

The Insufficient Heap Memory alarm (critical) indicates that there is insufficient heap memory. To troubleshoot and correct the cause of the Insufficient Heap Memory alarm, refer to the [“Insufficient Heap Memory - Signaling \(81\) \(H.323\)” section on page 10-115](#).

## Insufficient Shared Memory Pools - Signaling (82) (H.323)

The Insufficient Shared Memory Pools alarm (critical) indicates that there is insufficient shared memory pools. To troubleshoot and correct the cause of the Insufficient Shared Memory Pools alarm, refer to the [“Insufficient Shared Memory Pools - Signaling \(82\) \(H.323\)” section on page 10-115](#).

## Error While Binding to Socket - Signaling (83)

The Error While Binding to Socket alarm (critical) indicates that an error occurred while binding to the socket. To troubleshoot and correct the cause of the Error While Binding to Socket alarm, refer to the [“Error While Binding to Socket - Signaling \(83\)” section on page 10-115](#).

## Reached Maximum Socket Limit - Signaling (84) (H.323)

The Reached Maximum Socket Limit alarm (critical) indicates that the Cisco BTS 10200 Softswitch system has reached the maximum socket limit. To troubleshoot and correct the cause of the Reached Maximum Socket Limit alarm, refer to the [“Reached Maximum Socket Limit - Signaling \(84\) \(H.323\)” section on page 10-115](#).

## Initialization Failure - Signaling (85)

The Initialization Failure alarm (critical) indicates that the Cisco BTS 10200 Softswitch system failed to initialize. To troubleshoot and correct the cause of the Initialization Failure alarm, refer to the [“Initialization Failure - Signaling \(85\)” section on page 10-116](#).

## Remote H323 Gateway is not Reachable - Signaling (86) (H.323)

The Remote H323 Gateway is not Reachable alarm (major) indicates that the remote H323 gateway is not reachable. To troubleshoot and correct the cause of the Remote H323 Gateway is not Reachable alarm, refer to the [“Remote H323 Gateway is not Reachable - Signaling \(86\) \(H.323\)”](#) section on page 10-116.

## H323 Message Parsing Error - Signaling (87) (H.323)

The H323 Message Parsing Error alarm (major) indicates that a H323 message parsing error has occurred. To troubleshoot and correct the cause of the H323 Message Parsing Error alarm, refer to the [“H323 Message Parsing Error - Signaling \(87\) \(H.323\)”](#) section on page 10-116.

## H323 Message Encoding Error - Signaling (88) (H.323)

The H323 Message Encoding Error alarm (major) indicates that a H323 message encoding error has occurred. To troubleshoot and correct the cause of the H323 Message Encoding Error alarm, refer to the [“H323 Message Encoding Error - Signaling \(88\) \(H.323\)”](#) section on page 10-116.

## Gatekeeper not Available/Reachable - Signaling (89)

The Gatekeeper not Available/Reachable alarm (major) indicates that the gatekeeper is not available or the gatekeeper is not reachable. To troubleshoot and correct the cause of the Gatekeeper not Available/Reachable alarm, refer to the [“Gatekeeper not Available/Reachable - Signaling \(89\)”](#) section on page 10-116.

## Alternate Gatekeeper is not Responding - Signaling (90)

The Alternate Gatekeeper is not Responding alarm (major) indicates that the alternate gatekeeper is not responding. To troubleshoot and correct the cause of the Alternate Gatekeeper is not Responding alarm, refer to the [“Alternate Gatekeeper is not Responding - Signaling \(90\)”](#) section on page 10-117.

## Endpoint Security Violation - Signaling (91) (H.323)

The Endpoint Security Violation alarm (major) indicates that an H323 security violation has occurred. To troubleshoot and correct the cause of the Endpoint Security Violation alarm, refer to the [“Endpoint Security Violation - Signaling \(91\) \(H.323\)”](#) section on page 10-117.

## Invalid Call Identifier - Signaling (92)

The Invalid Call Identifier alarm (minor) indicates that the Call ID was invalid or changed mid-call. To troubleshoot and correct the cause of the Invalid Call Identifier alarm, refer to the [“Invalid Call Identifier - Signaling \(92\)”](#) section on page 10-117.

## Invalid Call Reference Value - Signaling (93)

The Invalid Call Reference Value alarm (minor) indicates that the Call ID was invalid or changed mid-call. To troubleshoot and correct the cause of the Invalid Call Reference Value alarm, refer to the [“Invalid Call Reference Value - Signaling \(93\)” section on page 10-117](#).

## Invalid Conference Identifier - Signaling (94)

The Invalid Conference Identifier alarm (minor) indicates that the Call ID was invalid or changed mid-call. To troubleshoot and correct the cause of the Invalid Conference Identifier alarm, refer to the [“Invalid Conference Identifier - Signaling \(94\)” section on page 10-117](#).

## Invalid Message from the Network - Signaling (95)

The Invalid Message from the Network alarm (minor) indicates that an unsupported or invalid message type was received from network. To troubleshoot and correct the cause of the Invalid Message from the Network alarm, refer to the [“Invalid Message from the Network - Signaling \(95\)” section on page 10-118](#).

## Internal Call Processing Error - Signaling (96)

The Internal Call Processing Error alarm (minor) indicates that an internal call processing error has occurred. To troubleshoot and correct the cause of the Internal Call Processing Error alarm, refer to the [“Internal Call Processing Error - Signaling \(96\)” section on page 10-118](#).

## Insufficient Information to Complete Call - Signaling (97)

The Insufficient Information to Complete Call alarm (minor) indicates that there was insufficient information to complete a call. To troubleshoot and correct the cause of the Insufficient Information to Complete Call alarm, refer to the [“Insufficient Information to Complete Call - Signaling \(97\)” section on page 10-118](#).

## H323 Protocol Inconsistencies - Signaling (98) (H.323)

The H323 Protocol Inconsistencies alarm (minor) indicates that the H323 endpoint and Cisco BTS 10200 Softswitch are running different protocol versions. To troubleshoot and correct the cause of the H323 Protocol Inconsistencies alarm, refer to the [“H323 Protocol Inconsistencies - Signaling \(98\) \(H.323\)” section on page 10-118](#).

## Abnormal Call Clearing - Signaling (99)

The Abnormal Call Clearing alarm (minor) indicates that an unsupported or invalid message type was received from network. To troubleshoot and correct the cause of the Abnormal Call Clearing alarm, refer to the [“Abnormal Call Clearing - Signaling \(99\)” section on page 10-118](#).



## Codec Negotiation Failed - Signaling (100)

The Codec Negotiation Failed alarm (minor) indicates that the codec negotiation has failed. To troubleshoot and correct the cause of the Codec Negotiation Failed alarm, refer to the [“Codec Negotiation Failed - Signaling \(100\)”](#) section on page 10-119.

## Per Call Security Violation - Signaling (101)

The Per Call Security Violation alarm (minor) indicates that a call security violation has occurred. To troubleshoot and correct the cause of the Per Call Security Violation alarm, refer to the [“Per Call Security Violation - Signaling \(101\)”](#) section on page 10-119.

## H323 Network Congested - Signaling (102) (H.323)

The H323 Network Congested alarm indicates (minor) that the H323 application process has depleted its resources and no more calls can be completed. To troubleshoot and correct the cause of the H323 Network Congested alarm, refer to the [“H323 Network Congested - Signaling \(102\) \(H.323\)”](#) section on page 10-119.

## Aggregation Connection Down - Signaling (103)

The Aggregation Connection Down alarm (major) indicates that the aggregation (AGGR) TCP connection is down. To troubleshoot and correct the cause of the Aggregation Connection Down alarm, refer to the [“Aggregation Connection Down - Signaling \(103\)”](#) section on page 10-119.

## Aggregation Unable To Establish Connection - Signaling (104)

The Aggregation Unable To Establish Connection event functions as an informational alert that the AGGR is unable to establish a connection. The primary cause of the event is that the TCP connection failed to establish. To correct the primary cause of the event, check the IP Connectivity of CA and CMTS.

## Aggregation Gate Set Failed - Signaling (105)

The Aggregation Gate Set Failed event functions as an informational alert that the AGGR gate set failed. The primary cause of the event is that the gate set acknowledgement never came from the CMTS. The event is informational and no further action is required.

## Enhanced Subscriber Authentication Cisco BTS 10200 Softswitch Delivery Function Connection Down - Signaling (106)

The Enhanced Subscriber Authentication Cisco BTS 10200 Softswitch Delivery Function Connection Down alarm (minor) indicates that the enhanced subscriber authentication (ESA) Cisco BTS 10200 Softswitch DF connection is down. To troubleshoot and correct the cause of the Enhanced Subscriber Authentication Cisco BTS 10200 Softswitch Delivery Function Connection Down alarm, refer to the [“Enhanced Subscriber Authentication Cisco BTS 10200 Softswitch Delivery Function Connection Down - Signaling \(106\)”](#) section on page 10-119.

## Logical Internet Protocol Addresses not Mapped Correctly - Signaling (107)

The Logical Internet Protocol Addresses not Mapped Correctly alarm (critical) indicates that the logical IP addresses are not mapped correctly. To troubleshoot and correct the cause of the Logical Internet Protocol Addresses not Mapped Correctly alarm, refer to the [“Logical Internet Protocol Addresses not Mapped Correctly - Signaling \(107\)”](#) section on page 10-120.

## Current SIA Configuration only Valid for Simplex Systems - Signaling (108)

The Current SIA Configuration only Valid for Simplex Systems alarm (major) indicates that the Cisco BTS 10200 Softswitch system can only operate in the simplex mode. To troubleshoot and correct the cause of the Current SIA Configuration only Valid for Simplex Systems alarm, refer to the [“Current SIA Configuration only Valid for Simplex Systems - Signaling \(108\)”](#) section on page 10-120.

## Stream Control Transmission Protocol Association Failure - Signaling (109)

The Stream Control Transmission Protocol Association Failure alarm (major) indicates that the SCTP association failed. To troubleshoot and correct the cause of the Stream Control Transmission Protocol Association Failure alarm, refer to the [“Stream Control Transmission Protocol Association Failure - Signaling \(109\)”](#) section on page 10-121.

## Signaling Gateway Group is Out-of-Service - Signaling (110)

The Signaling Gateway Group is Out-of-Service alarm (major) indicates that the signaling gateway group is out-of-service. To troubleshoot and correct the cause of the Signaling Gateway Group is Out-of-Service alarm, refer to the [“Signaling Gateway Group Is Out-of-Service - Signaling \(110\)”](#) section on page 10-125.

## Stream Control Transmission Protocol Association Degraded (One of Two Internet Protocol Connections Down) - Signaling (111)

The Stream Control Transmission Protocol Association Degraded (One of Two Internet Protocol Connections Down) alarm (major) indicates that the SCTP association is degraded. To troubleshoot and correct the cause of the Stream Control Transmission Protocol Association Degraded (One of Two Internet Protocol Connections Down) alarm, refer to the [“Stream Control Transmission Protocol Association Degraded \(One of Two Internet Protocol Connections Down\) - Signaling \(111\)”](#) section on page 10-125.

## Stream Control Transmission Protocol Association Configuration Error - Signaling (112)

The Stream Control Transmission Protocol Association Configuration Error alarm (minor) indicates that a SCTP association configuration error has occurred. To troubleshoot and correct the cause of the Stream Control Transmission Protocol Association Configuration Error alarm, refer to the [“Stream Control Transmission Protocol Association Configuration Error - Signaling \(112\)”](#) section on page 10-126.

## Signaling Gateway Failure - Signaling (113)

The Signaling Gateway Failure alarm (major) indicates that all associated signaling gateway processes are out-of-service. To troubleshoot and correct the cause of the Signaling Gateway Failure alarm, refer to the [“Signaling Gateway Failure - Signaling \(113\)”](#) section on page 10-126.

## Signaling Gateway Process is Out-of-Service - Signaling (114)

The Signaling Gateway Process is Out-of-Service alarm (major) indicates that all SCTP associations between the SGP and the CA are out-of-service. To troubleshoot and correct the cause of the Signaling Gateway Process is Out-of-Service alarm, refer to the [“Signaling Gateway Process Is Out-of-Service - Signaling \(114\)”](#) section on page 10-127.

## Invalid Routing Context Received - Signaling (115)

The Invalid Routing Context Received event serves as a warning that an invalid routing context was received. The primary cause of the event is that the routing context was configured improperly on the CA or the SG. To correct the primary cause of the event, reconfigure the routing context on the CA or the SG so that the routing context matches in both places.

## Destination Point Code User Part Unavailable - Signaling (116)

The Destination Point Code User Part Unavailable alarm (major) indicates that a layer 4 user part, such as ISUP, is unavailable at the DPC in the SS7 network. To troubleshoot and correct the cause of the Destination Point Code User Part Unavailable alarm, refer to the [“Destination Point Code User Part Unavailable - Signaling \(116\)”](#) section on page 10-127.

## Circuit Validation Test Message Received for an Unequipped Circuit Identification Code - Signaling (117)

The Circuit Validation Test Message Received for an Unequipped Circuit Identification Code alarm (minor) indicates that a CVT message was received for an unequipped CIC. To troubleshoot and correct the cause of the Circuit Validation Test Message Received for an Unequipped Circuit Identification Code alarm, refer to the [“Circuit Validation Test Message Received for an Unequipped Circuit Identification Code - Signaling \(117\)”](#) section on page 10-127.

## Circuit Verification Response Received with Failed Indication - Signaling (118)

The Circuit Verification Response Received with Failed Indication alarm (minor) indicates that a circuit verification response (CVR) message was received with a failure indication. To troubleshoot and correct the cause of the Circuit Verification Response Received with Failed Indication alarm, refer to the [“Circuit Verification Response Received with Failed Indication - Signaling \(118\)”](#) section on page 10-127.

## Signaling System 7 Adapter Process Faulty - Signaling (119)

The Signaling System 7 Adapter Process Faulty alarm (critical) indicates that a S7A process is faulty. To troubleshoot and correct the cause of the Signaling System 7 Adapter Process Faulty alarm, refer to the [“S7A Process Faulty - Signaling \(119\)”](#) section on page 10-116.

## Signaling System 7 Module/Signaling System 7 Adapter Faulty - Signaling (120)

The Signaling System 7 Module/Signaling System 7 Adapter Faulty alarm (critical) indicates that the S7M/S7A processes are faulty. To troubleshoot and correct the cause of the Signaling System 7 Module/Signaling System 7 Adapter Faulty alarm, refer to the [“S7M/S7A Faulty - Signaling \(120\)”](#) section on page 10-116.

## Message Transfer Part 3 User Adapter Cannot Go Standby - Signaling (121)

The Message Transfer Part 3 User Adapter Cannot Go Standby alarm (major) indicates that the M3UA process cannot go into standby mode. To troubleshoot and correct the cause of the Message Transfer Part 3 User Adapter Cannot Go Standby alarm, refer to the [“Message Transfer Part 3 User Adapter Cannot Go Standby - Signaling \(121\)”](#) section on page 10-128.

## Message Transfer Part 3 User Adapter Cannot Go Active - Signaling (122)

The Message Transfer Part 3 User Adapter Cannot Go Active alarm (major) indicates that the M3UA process cannot go into active mode. To troubleshoot and correct the cause of the Message Transfer Part 3 User Adapter Cannot Go Active alarm, refer to the [“Message Transfer Part 3 User Adapter Cannot Go Active - Signaling \(122\)”](#) section on page 10-128.

## Remote Subsystem is out of Service - Signaling (124)

The Remote Subsystem is out of Service alarm (minor) indicates that the remote subsystem is out-of-service. To troubleshoot and correct the cause of the Remote Subsystem is out of Service alarm, refer to the [“Remote Subsystem is Out Of Service - Signaling \(124\)”](#) section on page 10-128.

## Signaling Connection Control Part Routing Error - Signaling (125)

The Signaling Connection Control Part Routing Error alarm (major) indicates that the SCCP route was invalid or not available. To troubleshoot and correct the cause of the Signaling Connection Control Part Routing Error alarm, refer to the [“Signaling Connection Control Part Routing Error - Signaling \(125\)”](#) section on page 10-129.

## Signaling Connection Control Binding Failure - Signaling (126)

The Signaling Connection Control Binding Failure alarm (major) indicates that the SCCP binding failed. To troubleshoot and correct the cause of the Signaling Connection Control Binding Failure alarm, refer to the [“Signaling Connection Control Part Binding Failure - Signaling \(126\)”](#) section on page 10-129.

## Transaction Capabilities Application Part Binding Failure - Signaling (127)

The Transaction Capabilities Application Part Binding Failure alarm (major) indicates that the TCAP binding failed. To troubleshoot and correct the cause of the Transaction Capabilities Application Part Binding Failure alarm, refer to the [“Transaction Capabilities Application Part Binding Failure - Signaling \(127\)”](#) section on page 10-129.

## Transaction Capabilities Application Part Reaches the Provisioned Resource Limit - Signaling (132)

The Transaction Capabilities Application Part Reaches the Provisioned Resource Limit event serves as a warning that the TCAP process has reached or reaches the provisioned resource limit. The primary cause of the event is that the TCAP process runs out of all of the pre-configured dialogue IDs or invoke IDs. To correct the primary cause of the event, increase the number pre-configured dialogue IDs or invoke IDs.

## Unable to Decode Generic Transport Descriptor Message - Signaling (133)

The Unable to Decode Generic Transport Descriptor Message event functions as an informational alert that a GTD message could not be decoded. The primary cause of the event is that the GTD parser failed to decode a GTD message received from the specified endpoint. To correct the primary cause of the event, verify that the version of the GTD protocol used by the device at the remote endpoint is consistent with the version expected by the call agent. Examine the associated signaling link to see if there is any interruption of the supplementary services on the link.

## Signaling System 7 Message Encoding Failure - Signaling (134)

The Signaling System 7 Message Encoding Failure event functions as an informational alert that a SS7 message encoding failed. The primary cause of the event is that there was an error in the ISUP stack or the SAI message. To correct the primary cause of the event, capture a SS7 trace of the circuit for examination by Cisco TAC. Refer to the [“Obtaining Technical Assistance” section on page xxxviii](#) for detailed instructions on contacting Cisco TAC and opening a service request.

## Signaling System 7 Message Decoding Failure - Signaling (135)

The Signaling System 7 Message Decoding Failure event functions as an informational alert that the decoding of a SS7 message failed. The primary cause of the event is that an error occurred in the ISUP stack or the SAI message. To correct the primary cause of the event, capture a SS7 trace of the circuit for examination by Cisco TAC. Refer to the [“Obtaining Technical Assistance” section on page xxxviii](#) for detailed instructions on contacting Cisco TAC and opening a service request.

## Signaling System 7 Message Invalid Received - Signaling (136)

The Signaling System 7 Message Invalid Received event functions as an informational alert that an invalid SS7 message was received. The primary cause of the event is that an invalid message was received from the line in the ISUP stack. To correct the primary cause of the event, verify the SSP sending the message to the CA is correctly configured. Capture a SS7 trace of the circuit for examination by Cisco TAC. Refer to the [“Obtaining Technical Assistance” section on page xxxviii](#) for detailed instructions on contacting Cisco TAC and opening a service request.

## Signaling System 7 Confusion Message Received - Signaling (137)

The Signaling System 7 Confusion Message Received event functions as an informational alert that the received SS7 message was confused. The primary cause of the event is that an ISUP message or parameter received was not recognized or understood. To correct the primary cause of the event, check the log for more information (including CFN diagnostic output). Capture SS7 trace of affected circuits. If diagnostic data indicates messages/parameters that must be supported are being dropped, refer the captured data to Cisco TAC along with a description of the call scenario. Refer to the [“Obtaining Technical Assistance” section on page xxxviii](#) for detailed instructions on contacting Cisco TAC and opening a service request.

## Number of Open Session Initiation Protocol Connections is Reaching Engineered Limit - Signaling (138)

The Number of Open Session Initiation Protocol Connections is Reaching Engineered Limit alarm (minor) indicates that the number of open SIP connections is reaching the engineered limit. To troubleshoot and correct the cause of the Number of Open Session Initiation Protocol Connections is Reaching Engineered Limit alarm, refer to the [“Number of Open Session Initiation Protocol Connections is Reaching Engineered Limit - Signaling \(138\)” section on page 129](#).

## Signaling System 7 Trunk was Found to be in Erroneous State - Signaling (139) (SS7)

The Signaling System 7 Trunk was Found to be in Erroneous State event functions as an informational alert that a SS7 trunk was found to be in an erroneous state. The primary cause of the event is that a discrepancy exists between the local and the remote trunk states. The corrective action is automatically enforced when using ANSI ISUP.

## Unanswered Information Message - Signaling (140)

The Unanswered Information Message event functions as an informational alert that an INF message has not been answered. The primary cause of the event is that the far-end switch is not responding to INF message with an INR message. To correct the primary cause of the event, verify that the far-end switch can correctly respond to an INF message.

## Address not Resolved by Domain Name System Server - Signaling (141)

The Address not Resolved by Domain Name System Server event serves as a warning that an address was not resolved by the DNS server. The primary cause of the event is that the TSAP address/hostname is not defined in the DNS. To correct the primary cause of the event, add an entry for TSAP address to the DNS server or fix the Cisco BTS 10200 Softswitch provisioning.

## Session Initiation Protocol Trunk Operationally Out-of-Service - Signaling (142)

The Session Initiation Protocol Trunk Operationally Out-of-Service alarm (critical) indicates that the SIP trunk is operationally out-of-service. To troubleshoot and correct the cause of the Session Initiation Protocol Trunk Operationally Out-of-Service alarm, refer to the [“Session Initiation Protocol Trunk Operationally Out-of-Service - Signaling \(142\)”](#) section on page 10-129.

## Internet Protocol Interface Link to the Signaling System 7 Signaling Gateway is Down - Signaling (143)

The Internet Protocol Interface Link to the Signaling System 7 Signaling Gateway is Down alarm (minor) indicates that an IP interface link to the SS7 signaling gateway is down. To troubleshoot and correct the cause of the Internet Protocol Interface Link to the Signaling System 7 Signaling Gateway is Down alarm, refer to the [“Internet Protocol Interface Link to the Signaling System 7 Signaling Gateway is Down - Signaling \(143\)”](#) section on page 10-130.

## All Internet Interface Links to Signaling System 7 Signaling Gateway are Down - Signaling (144)

The All Internet Interface Links to Signaling System 7 Signaling Gateway are Down alarm (critical) indicates that all IP interface links to the SS7 signaling gateway are down. To troubleshoot and correct the cause of the All Internet Interface Links to Signaling System 7 Signaling Gateway are Down alarm, refer to the [“All Internet Protocol Interface Links to Signaling System 7 Signaling Gateway are Down - Signaling \(144\)”](#) section on page 10-130.

## One Internet Protocol Interface to Signaling System 7 Signaling Gateway is Down - Signaling (145)

The One Internet Protocol Interface to Signaling System 7 Signaling Gateway is Down alarm (minor) indicates that one IP interface link to the SS7 signaling gateway is down. To troubleshoot and correct the cause of the One Internet Protocol Interface to Signaling System 7 Signaling Gateway is Down alarm, refer to the [“One Internet Protocol Interface to Signaling System 7 Signaling Gateway is Down - Signaling \(145\)”](#) section on page 10-130.

## Stream Control Transmission Protocol Association Congested - Signaling (150)

The Stream Control Transmission Protocol Association Congested alarm (minor) indicates that the SCTP association is congested. To troubleshoot and correct the cause of the Stream Control Transmission Protocol Association Congested alarm, refer to the [“Stream Control Transmission Protocol Association Congested - Signaling \(150\)”](#) section on page 10-130.



# Troubleshooting Signaling Alarms

This section provides the information needed to monitor and correct Signaling alarms. [Table 10-3](#) lists all Signaling alarms in numerical order and provides cross reference to each subsection in this section.

**Table 10-3** *Cisco BTS 10200 Softswitch Signaling Alarms*

| Alarm Type    | Alarm Name                                                                                                                       | Alarm Severity |
|---------------|----------------------------------------------------------------------------------------------------------------------------------|----------------|
| SIGNALING(7)  | <a href="#">Socket Failure - Signaling (7)</a>                                                                                   | MAJOR          |
| SIGNALING(8)  | <a href="#">Session Initiation Protocol Message Receive Failure - Signaling (8)</a>                                              | MAJOR          |
| SIGNALING(9)  | <a href="#">Timeout on Internet Protocol Address - Signaling (9)</a>                                                             | MAJOR          |
| SIGNALING(10) | <a href="#">Failed to Send Complete Session Initiation Protocol Message - Signaling (10)</a>                                     | MINOR          |
| SIGNALING(11) | <a href="#">Failed to Allocate Session Initiation Protocol Control Block - Signaling (11)</a>                                    | MAJOR          |
| SIGNALING(12) | <a href="#">Feature Server is not Up or is not Responding to Call Agent - Signaling (12)</a>                                     | CRITICAL       |
| SIGNALING(13) | <a href="#">Signaling System 7 Signaling Link Down - Signaling (13)</a>                                                          | MAJOR          |
| SIGNALING(14) | <a href="#">Link is Remotely Inhibited - Signaling (14)</a>                                                                      | MINOR          |
| SIGNALING(15) | <a href="#">Link is Locally Inhibited - Signaling (15)</a>                                                                       | MINOR          |
| SIGNALING(16) | <a href="#">Link is Congested - Signaling (16)</a>                                                                               | MINOR          |
| SIGNALING(17) | <a href="#">Link: Local Processor Outage - Signaling (17)</a>                                                                    | MINOR          |
| SIGNALING(18) | <a href="#">Link: Remote Processor Outage - Signaling (18)</a>                                                                   | MINOR          |
| SIGNALING(19) | <a href="#">Link Set Inaccessible - Signaling (19)</a>                                                                           | MAJOR          |
| SIGNALING(20) | <a href="#">Link Set Congestion - Signaling (20)</a>                                                                             | MAJOR          |
| SIGNALING(21) | <a href="#">Route Set Failure - Signaling (21)</a>                                                                               | MAJOR          |
| SIGNALING(22) | <a href="#">Route Set Congested - Signaling (22)</a>                                                                             | MINOR          |
| SIGNALING(23) | <a href="#">Destination Point Code Unavailable - Signaling (23)</a>                                                              | MAJOR          |
| SIGNALING(24) | <a href="#">Destination Point Code Congested - Signaling (24)</a>                                                                | MINOR          |
| SIGNALING(36) | <a href="#">Trunk Locally Blocked - Signaling (36)</a>                                                                           | MINOR          |
| SIGNALING(40) | <a href="#">Trunk Remotely Blocked - Signaling (40)</a>                                                                          | MAJOR          |
| SIGNALING(59) | <a href="#">Auto State Change for Integrated Services Digital Network Trunk Group by Media Gateway - Signaling (59)</a>          | MAJOR          |
| SIGNALING(63) | <a href="#">Media Gateway/Termination Faulty - Signaling (63)</a>                                                                | MAJOR          |
| SIGNALING(64) | <a href="#">Media Gateway Adapter Running out of Shared Memory Pools - Signaling (64)</a>                                        | CRITICAL       |
| SIGNALING(65) | <a href="#">Media Gateway Adapter Running out of Heap Memory - Signaling (65)</a>                                                | CRITICAL       |
| SIGNALING(66) | <a href="#">Call Agent Internal Error (Because of Which Media Gateway Adapter has to Start Automatically) - Signaling (66)</a>   | MAJOR          |
| SIGNALING(68) | <a href="#">Media Gateway or Termination are Found Administratively Out of Service - Signaling (68)</a>                          | MAJOR          |
| SIGNALING(69) | <a href="#">Call Agent and Feature Server Communication Message Timeout - Signaling (69)</a>                                     | CRITICAL       |
| SIGNALING(75) | <a href="#">Signaling System 7 Stack not Ready - Signaling (75)</a>                                                              | CRITICAL       |
| SIGNALING(78) | <a href="#">Integrated Services Digital Network Single D-channel Down for Non-Facility Associated Signaling - Signaling (78)</a> | MINOR          |

**Table 10-3** *Cisco BTS 10200 Softswitch Signaling Alarms (continued)*

| Alarm Type     | Alarm Name                                                                                                                  | Alarm Severity |
|----------------|-----------------------------------------------------------------------------------------------------------------------------|----------------|
| SIGNALING(79)  | Media Gateway Unreachable - Signaling (79)                                                                                  | MAJOR          |
| SIGNALING(80)  | Out of Bounds, Memory/Socket Error - Signaling (80)                                                                         | CRITICAL       |
| SIGNALING(81)  | Insufficient Heap Memory - Signaling (81) (H.323)                                                                           | CRITICAL       |
| SIGNALING(82)  | Insufficient Shared Memory Pools - Signaling (82) (H.323)                                                                   | CRITICAL       |
| SIGNALING(83)  | Error While Binding to Socket - Signaling (83)                                                                              | CRITICAL       |
| SIGNALING(84)  | Reached Maximum Socket Limit - Signaling (84) (H.323)                                                                       | CRITICAL       |
| SIGNALING(85)  | Initialization Failure - Signaling (85)                                                                                     | CRITICAL       |
| SIGNALING(86)  | Remote H323 Gateway is not Reachable - Signaling (86) (H.323)                                                               | MAJOR          |
| SIGNALING(87)  | H323 Message Parsing Error - Signaling (87) (H.323)                                                                         | MAJOR          |
| SIGNALING(88)  | H323 Message Encoding Error - Signaling (88) (H.323)                                                                        | MAJOR          |
| SIGNALING(89)  | Gatekeeper not Available/Reachable - Signaling (89)                                                                         | MAJOR          |
| SIGNALING(90)  | Alternate Gatekeeper is not Responding - Signaling (90)                                                                     | MAJOR          |
| SIGNALING(91)  | Endpoint Security Violation - Signaling (91) (H.323)                                                                        | MAJOR          |
| SIGNALING(92)  | Invalid Call Identifier - Signaling (92)                                                                                    | MINOR          |
| SIGNALING(93)  | Invalid Call Reference Value - Signaling (93)                                                                               | MINOR          |
| SIGNALING(94)  | Invalid Conference Identifier - Signaling (94)                                                                              | MINOR          |
| SIGNALING(95)  | Invalid Message from the Network - Signaling (95)                                                                           | MINOR          |
| SIGNALING(96)  | Internal Call Processing Error - Signaling (96)                                                                             | MINOR          |
| SIGNALING(97)  | Insufficient Information to Complete Call - Signaling (97)                                                                  | MINOR          |
| SIGNALING(98)  | H323 Protocol Inconsistencies - Signaling (98) (H.323)                                                                      | MINOR          |
| SIGNALING(99)  | Abnormal Call Clearing - Signaling (99)                                                                                     | MINOR          |
| SIGNALING(100) | Codec Negotiation Failed - Signaling (100)                                                                                  | MINOR          |
| SIGNALING(101) | Per Call Security Violation - Signaling (101)                                                                               | MINOR          |
| SIGNALING(102) | H323 Network Congested - Signaling (102) (H.323)                                                                            | MINOR          |
| SIGNALING(103) | Aggregation Connection Down - Signaling (103)                                                                               | MAJOR          |
| SIGNALING(106) | Enhanced Subscriber Authentication Cisco BTS 10200 Softswitch Delivery Function Connection Down - Signaling (106)           | MINOR          |
| SIGNALING(107) | Logical Internet Protocol Addresses not Mapped Correctly - Signaling (107)                                                  | CRITICAL       |
| SIGNALING(108) | Current SIA Configuration only Valid for Simplex Systems - Signaling (108)                                                  | MAJOR          |
| SIGNALING(109) | Stream Control Transmission Protocol Association Degraded (One of Two Internet Protocol Connections Down) - Signaling (111) | MAJOR          |
| SIGNALING(110) | Signaling Gateway Group Is Out-of-Service - Signaling (110)                                                                 | CRITICAL       |
| SIGNALING(111) | Stream Control Transmission Protocol Association Degraded (One of Two Internet Protocol Connections Down) - Signaling (111) | MINOR          |
| SIGNALING(112) | Stream Control Transmission Protocol Association Configuration Error - Signaling (112)                                      | MINOR          |
| SIGNALING(113) | Signaling Gateway Failure - Signaling (113)                                                                                 | MAJOR          |

**Table 10-3** *Cisco BTS 10200 Softswitch Signaling Alarms (continued)*

| Alarm Type     | Alarm Name                                                                                                                  | Alarm Severity |
|----------------|-----------------------------------------------------------------------------------------------------------------------------|----------------|
| SIGNALING(114) | Stream Control Transmission Protocol Association Degraded (One of Two Internet Protocol Connections Down) - Signaling (111) | MAJOR          |
| SIGNALING(114) | Signaling Gateway Process Is Out-of-Service - Signaling (114)                                                               | MAJOR          |
| SIGNALING(116) | Destination Point Code User Part Unavailable - Signaling (116)                                                              | MAJOR          |
| SIGNALING(117) | Circuit Validation Test Message Received for an Unequipped Circuit Identification Code - Signaling (117)                    | MINOR          |
| SIGNALING(118) | Circuit Verification Response Received with Failed Indication - Signaling (118)                                             | MINOR          |
| SIGNALING(119) | Signaling System 7 Adapter Process Faulty - Signaling (119)                                                                 | CRITICAL       |
| SIGNALING(120) | Signaling System 7 Module/Signaling System 7 Adapter Faulty - Signaling (120)                                               | CRITICAL       |
| SIGNALING(121) | Message Transfer Part 3 User Adapter Cannot Go Standby - Signaling (121)                                                    | MAJOR          |
| SIGNALING(122) | Message Transfer Part 3 User Adapter Cannot Go Active - Signaling (122)                                                     | MAJOR          |
| SIGNALING(124) | Remote Subsystem is Out Of Service - Signaling (124)                                                                        | MINOR          |
| SIGNALING(125) | Signaling Connection Control Part Routing Error - Signaling (125)                                                           | MAJOR          |
| SIGNALING(126) | Signaling Connection Control Part Binding Failure - Signaling (126)                                                         | MAJOR          |
| SIGNALING(127) | Transaction Capabilities Application Part Binding Failure - Signaling (127)                                                 | MAJOR          |
| SIGNALING(138) | Number of Open Session Initiation Protocol Connections is Reaching Engineered Limit - Signaling (138)                       | MINOR          |
| SIGNALING(142) | Session Initiation Protocol Trunk Operationally Out-of-Service - Signaling (142)                                            | CRITICAL       |
| SIGNALING(143) | Internet Protocol Interface Link to the Signaling System 7 Signaling Gateway is Down - Signaling (143)                      | MINOR          |
| SIGNALING(144) | All Internet Protocol Interface Links to Signaling System 7 Signaling Gateway are Down - Signaling (144)                    | CRITICAL       |
| SIGNALING(145) | One Internet Protocol Interface to Signaling System 7 Signaling Gateway is Down - Signaling (145)                           | MINOR          |
| SIGNALING(149) | Stream Control Transmission Protocol Association Congested - Signaling (150)                                                | MAJOR          |
| SIGNALING(150) | Stream Control Transmission Protocol Association Congested - Signaling (150)                                                | MINOR          |

## Socket Failure - Signaling (7)

The Socket Failure alarm (major) indicates that there is a failure in creating the UDP port used by the MGCP stacks. The primary cause of the alarm there is a failure in creating the UDP port used by the MGCP stacks. To correct the primary cause of the alarm, reconfigure the MGCP stack to use a free UDP port. The secondary cause of the alarm is that some other application may already be active on the same UDP port and IP address to which the Call Agent MGCP stack is assigned.

### Media Gateway Control Protocol

The Socket Failure alarm is issued when there is a failure in creating the UDP port used by the MGCP stacks. Some other application may already be active on the same UDP port and IP address to which the Call Agent MGCP stack is assigned. Reconfigure the MGCP stack to use a free UDP port.

### Session Initiation Protocol

The Socket Failure alarm is issued when there is a failure in creating the UDP port used by the SIA process. Some other application may already be active on the same UDP port and IP address to which the SIA process is assigned. Reconfigure the SIA port to use a free port or the SIP default port 5060.

## Session Initiation Protocol Message Receive Failure - Signaling (8)

The Session Initiation Protocol Message Receive Failure alarm (major) indicates that a SIP message receive has failed. The primary cause of the alarm is that Operating System level network errors have occurred or the network configuration is invalid. To correct the primary cause of the alarm, have the network administrator resolve the network errors. Contact Cisco TAC if you need assistance. Manually clear alarm. Restart this call agent instance using the platform start command. Refer to the [“Obtaining Technical Assistance”](#) section on page xxxviii for detailed instructions on contacting Cisco TAC and opening a service request.

### Session Initiation Protocol

The SIP Message Receive Failure alarm is issued when SIP messages cannot be received. This could be due to port conflict (two processes attempting to use the same UDP port). Examine the “HOSTNAME” field in the alarm report to determine the IP address or domain name of the Call Agent that generated this alarm. Telnet into this Call Agent instance as a root user. In this Call Agent, configure another UDP port for the SIA process to avoid port conflict, by setting the SIA port in platform.cfg file to another port number. Call Cisco TAC if you need assistance. Restart this Call Agent instance using the platform start command.

## Timeout on Internet Protocol Address - Signaling (9)

The Timeout on Internet Protocol Address alarm (major) indicates that an IP address has timed out. The alarm is issued when the OptiCall is unable to communicate with a gateway. To correct the primary cause of the alarm, verify that the gateway is both configured for service and that it has been set in service. Attempt to ping the gateway using the IP address from the Event Report. If the ping is not successful, then diagnose the issue that prevents the address from being reached. Use the Status MGW ID=xxx, where xxx is the IP address given in the Event Report. If the status is not INS, then use control mgw command to put it in service.

## Media Gateway Control Protocol

The Timeout on IP Address alarm is issued when the Cisco BTS 10200 Softswitch is unable to communicate with a gateway. Verify that the gateway is both configured for service and that it has been set in service. Attempt to ping the gateway using the IP address from the Event Report. If the ping is not successful, then diagnose the issue that prevents the address from being reached. Use the Status MGW ID=xxx, where xxx is the IP address given in the Event Report. If the status is not INS, then use the **control mgw** command to put it in service.

## Session Initiation Protocol

The Timeout on IP Address alarm is issued when the Call Agent did not receive SIP response messages from Call Agent specified in the Event Report. The Call Agent has already taken the necessary action to handle this situation by re-sending the SIP messages to the redundant IP address of the remote Call Agent.

## Failed to Send Complete Session Initiation Protocol Message - Signaling (10)

The Failed to Send Complete Session Initiation Protocol Message alarm (minor) indicates that a SIP message failure has occurred. The primary cause of the alarm is that the SIP stack failed to send an SIP message due to it exceeding the maximum length of a UDP packet. To correct the primary cause of the alarm, the message should be captured on passive testing equipment and sent to Cisco TAC for evaluation if that alarm occurred during normal network operations. Refer to the [“Obtaining Technical Assistance” section on page xxxviii](#) for detailed instructions on contacting Cisco TAC and opening a service request.

## Failed to Allocate Session Initiation Protocol Control Block - Signaling (11)

The Failed to Allocate Session Initiation Protocol Control Block alarm (major) indicates that a SIP control block allocation failed. The primary cause of the alarm is that there is not enough memory to allocate a SIP Call Control Block. To correct the primary cause of the alarm, Increase the SIP CCB count specified in mem.cfg file and restart the Call Agent for the changes to take effect.

## Feature Server is not Up or is not Responding to Call Agent - Signaling (12)

The Feature Server is not Up or is not Responding to Call Agent alarm (critical) indicates that the feature server is not up or is not responding to the call agent server. The primary cause of the alarm is that the feature server platform is down or is not operating properly. To correct the primary cause of the alarm, restart the applicable feature server.

## Signaling System 7 Signaling Link Down - Signaling (13)

The Signaling System 7 Signaling Link Down alarm (major) indicates the SS7 signaling link is down. The primary cause of the alarm is that the SS7 trunk group may be out-of-service (OOS). To correct the primary cause of the alarm, use the control ss7-trunk-grp command to place the trunk group in service (INS). The secondary cause of the alarm is that the local Ulticom stack may be down. To correct the secondary cause of the alarm, run the Ulticom stack command again. The tertiary cause of the alarm is that the SS7 link may be disconnected or faulty. To correct the tertiary cause of the alarm, check the Ulticom local configuration. The subsequent cause of the alarm is that the remote SS7 signaling site may be down or incorrectly configured. To correct the subsequent cause of the alarm, check the Ulticom remote configuration.

### Signal System 7 and Call Agent Fail-over Interaction

When an ISUP SS7 signaling link goes into the link failure state, an Signaling System 7 Signaling Link Down alarm (13) is activated and the call-agent will begin a 120 second timer. When the SS7 signaling link is restored, in-progress calls are cleared if they were in a transient state, if an event occurred that required the sending of an ISUP message during the link failure, or if the 120 second timer has expired.

Should the call-agent fail-over for any reason, the state of the 120 second timer or any indication of a request for an outgoing message that could not be sent will not be preserved. If the signaling links are in the failure state on the stand-by side, the 120 second timer will be re-started; however, if the links should restore prior to that the timer expiry, any stable calls will NOT be cleared.

This applies should multiple fail-overs occur prior to eventual signaling link restoration. In these situations, if a call clearing event has been missed, any calls remaining up will be cleared by the normal ISUP network recovery and message retransmission mechanisms.

## Link is Remotely Inhibited - Signaling (14)

The Link is Remotely Inhibited alarm (minor) indicates that the SS7 link is inhibited at the remote end. The primary cause of the alarm is that the specified SS7 link is inhibited at the remote end. To correct the primary cause of the alarm, monitor events and alarms at the network level for any related to the specified SS7 link. Restorative actions need to be taken on the remote end.

## Link is Locally Inhibited - Signaling (15)

The Link is Locally Inhibited alarm (minor) indicates that the SS7 link is inhibited at the local end. The primary cause of the alarm is that the specified SS7 link is inhibited at the local end. To correct the primary cause of the alarm, verify that the SS7 signaling adapter process is running and that the SS7 interface card(s) are in service. If a component is found to be non-operational, restore it to service.

## Link is Congested - Signaling (16)

The Link is Congested alarm (minor) indicates that the SS7 link is congested. The primary cause of the alarm is that the specified SS7 link is experiencing congestion. To correct the primary cause of the alarm, monitor event reports at the network level to determine if the traffic load on the specified SS7 link is too high on the local end, or if the remote end is lagging in processing the traffic. Verify that the SS7 link has not degraded in quality. Verify that the traffic load has not become unbalanced if multiple SS7 links are used. Verify that local SS7 signaling adapter process is running normally.

## Link: Local Processor Outage - Signaling (17)

The Link: Local Processor Outage alarm (minor) indicates that the SS7 link has experienced a local processor outage. The primary cause of the alarm is that the specified SS7 link has experienced a processor outage. To correct the primary cause of the alarm, monitor the system for maintenance event reports associated with the signaling adapter or underlying platform instance that support the specified SS7 link. Verify that the process and or platform are restarted and returned to service.

## Link: Remote Processor Outage - Signaling (18)

The Link: Remote Processor Outage alarm (minor) indicates that the SS7 link has experienced a remote processor outage. The primary cause of the alarm is that the specified SS7 link has experienced a processor outage. To correct the primary cause of the alarm, monitor the network level event reports for any events associated with the processing complex used by the specified SS7 link. Verify that the SS7 link is returned to service.

## Link Set Inaccessible - Signaling (19)

The Link Set Inaccessible alarm (major) indicates that the specified SS7 link is inaccessible. The primary cause of the alarm is that the specified SS7 link set is inaccessible. To correct the primary cause of alarm, return the SS7 signaling adapter and the associated call agent platform to service if the SS7 signaling adapter is not running normally and the associated call agent platform is not active.

## Link Set Congestion - Signaling (20)

The Link Set Congestion alarm (major) indicates that the specified SS7 link set is congested. The primary cause of the alarm is that the specified SS7 link set is experiencing congestion. To correct the primary cause of the alarm, monitor the alarm and event reports at the network level to determine if the traffic load on the specified SS7 link set is too high on the local end, or if the remote end is lagging in processing the traffic. Verify that the SS7 link set has not degraded in quality. Verify that the traffic load has not become unbalanced if multiple SS7 link sets are used. Verify that local SS7 signaling adapter process is running normally.

## Route Set Failure - Signaling (21)

The Route Set Failure alarm (major) indicates that the specified route set has experienced a failure. The primary cause of the alarm is the specified route set has experienced a failure. To correct the primary cause of the alarm, verify that the processing complex supporting the route set is functional. Monitor event reports at the network level to determine the failing component and verify its restoral to service.

## Route Set Congested - Signaling (22)

The Route Set Congested alarm (minor) indicates that the specified route set is congested. The primary of the alarm is that the specified route set is experiencing congestion. To correct the primary cause of the alarm, monitor event reports at the network level to determine if the traffic load on the specified SS7 link set is too high on the local end, or if the remote end is lagging in processing the traffic. Verify that the SS7 link set has not degraded in quality. Verify that the traffic load has not become unbalanced if multiple SS7 link sets are used. Verify that local SS7 signaling adapter process is running normally.



## Destination Point Code Unavailable - Signaling (23)

The Destination Point Code Unavailable alarm (major) indicates that the specified DPC is not available. This alarm indicates that the Cisco BTS 10200 Softswitch is unable to communicate with the specified DPC in the SS7 network. Determine if the issue is a communication problem between the Cisco BTS 10200 Softswitch and the IP transfer point (ITP) or if it is related to communication problems between the ITP and the DPC by following these steps:

- 
- Step 1** Use the Cisco BTS 10200 Softswitch CLI `show alarm` command to determine if there is an active Signaling Gateway Group Out of Service alarm. This will occur if communication has been lost to at least one of the SGs in the SG-Group. If so, proceed to the [“Signaling Gateway Group Is Out-of-Service - Signaling \(110\)”](#) section on page 10-125. Otherwise, proceed to Step 2.
- Step 2** Determine if there is an M3UA Cannot Go Active alarm. This occurs if, at the time of startup or failover, the Cisco BTS 10200 Softswitch is not able to communicate with any of the SGs. If this is the case, proceed to the [“Message Transfer Part 3 User Adapter Cannot Go Active - Signaling \(122\)”](#) section on page 10-128. Otherwise, proceed to Step 3.
- Step 3** If you arrive at this step, there is probably communication between the Cisco BTS 10200 Softswitch and ITP at the M3UA and SCCP user adapter (SUA) layers, and a communication problem exists between the ITP and the unavailable DPC. To confirm this, log on to each ITP, get into enable mode, and enter **show cs7 route**. The output of this command tells you if the associated DPC is accessible or not from the ITP point of view and will look similar to the following:

```
va-2651-82#show cs7 route
Destination Prio Linkset Name Route

229.123.2/24 INACC 1 lset1chn UNAVAIL
```

This output indicates that DPC 229.123.2 is unavailable from the ITP point of view.

- Step 4** Determine if the problem is at the link level or at a higher level outage in the DPC by typing **show cs7 linkset**. If the ITP shows that the DPC is AVAIL, there is a mismatch between the ITP and Cisco BTS 10200 Softswitch. Please contact the Cisco TAC.
- Step 5** Check whether the DPC has been removed from the Cisco BTS 10200 Softswitch database. At the Cisco BTS 10200 Softswitch CLI prompt, enter **show call-ctrl-route** or **show sccp-route** and see if the DPC is in any of the routes. If not, the alarm was raised before the associated routes were deleted. If this is the case, manually clear the alarm.
- Step 6** If you still cannot determine the cause of the problem, contact the Cisco TAC.
-

## Destination Point Code Congested - Signaling (24)

The Destination Point Code Congested alarm (minor) alarm indicates that the specified DPC is congested. This alarm indicates that the DPC in the SS7 network is congested, i.e., is in a state where it has received more traffic than it can handle. This should be a temporary state. If the type of network is National, which is generally the case in the United States, there will also be a level of congestion associated with the alarm.

The ITP should continually communicate with the DPC in the SS7 network to determine if congestion has abated. If this alarm does not clear or keeps reappearing after clearing, contact your SS7 service provider to determine why the DPC is congested.

The DPC Congested alarm is issued when the specified destination point code is congested. Monitor event reports at the network level to determine if the traffic load to the specified DPC is too high on the local end, or if the remote end is lagging in processing the traffic.

## Trunk Locally Blocked - Signaling (36)

The Trunk Locally Blocked alarm (minor) indicates that the trunk is locally blocked. The primary cause of the alarm is that a BLO or CGB message was sent on the specified CIC. For troubleshooting information, refer to [Appendix A, “System Usage of MGW Keepalive Parameters, Release 4.4.x.”](#)

## Trunk Remotely Blocked - Signaling (40)

The Trunk Remotely Blocked alarm (major) indicates that the trunk is remotely blocked. The primary cause of the alarm is that a BLO or CGB message was received on the specified CIC if it is SS7 trunk. Issued when SERVICE OOS message is received for ISDN trunks. Issued when Reverse Make Busy (rbz) signal is received for CAS operator trunk. No action is required. The system can be manually recovered from this condition locally by controlling the effected trunks to UEQP state and back INS.

## Auto State Change for Integrated Services Digital Network Trunk Group by Media Gateway - Signaling (59)

The Auto State Change for Integrated Services Digital Network Trunk Group by Media Gateway alarm (major) indicates that specified ISDN trunk group status was changed due to a media gateway operation. The primary cause of the alarm is that the specified ISDN trunk group's status was changed due to a media gateway operation. To correct the primary cause of the alarm, monitor the event reports at the network level to determine which media gateway caused the status change of the trunk group. Verify that the gateway is reconfigured properly to support the usage of the trunk group.

## Media Gateway/Termination Faulty - Signaling (63)

The Media Gateway/Termination Faulty alarm (major) indicates that a media gateway or termination has gone faulty due to the detection of an unknown endpoint, unknown package type, and unknown event, a hardware failure, or a general call agent error. The primary cause of the alarm is that a media gateway or termination has gone faulty due to the detection of an unknown endpoint, unknown package type, and unknown event (either a hardware failure or a general call agent error). To correct the primary cause of the alarm, verify the proper operation of the media gateway specified. Place the termination out-of-service and then back into service from the call agent.

## Media Gateway Adapter Running out of Shared Memory Pools - Signaling (64)

The Media Gateway Adapter Running out of Shared Memory Pools alarm (critical) indicates that the MGCP signaling adapter was unable to allocate data store for an IPC message due to a lack of resources. The primary cause of the alarm is that the MGCP signaling adapter was unable to allocate data store for an IPC message due to a lack of resources. To correct the primary cause of the alarm, contact Cisco TAC technologies for assistance. Refer to the [“Obtaining Technical Assistance”](#) section on page xxxviii for detailed instructions on contacting Cisco TAC and opening a service request.

## Media Gateway Adapter Running out of Heap Memory - Signaling (65)

The Media Gateway Adapter Running out of Heap Memory alarm (critical) indicates that the MGCP signaling adapter was unable to allocate data store for an IPC message from the heap due to a lack of resources. The primary cause of the alarm is that the MGCP signaling adapter was unable to allocate data store for an IPC message from the heap due to a lack of resources. To correct the primary cause of the alarm, contact Cisco TAC for assistance. Refer to the [“Obtaining Technical Assistance”](#) section on page xxxviii for detailed instructions on contacting Cisco TAC and opening a service request.

## Call Agent Internal Error (Because of Which Media Gateway Adapter has to Start Automatically) - Signaling (66)

The Call Agent Internal Error (Because of Which Media Gateway Adapter has to Start Automatically) alarm (major) indicates that a call agent internal error has occurred causing the restart of the MGCP signaling adapter. The primary cause of the alarm is that a call agent internal error has occurred causing the restart of the MGCP signaling adapter. To correct the primary cause of the alarm, send the log files to Cisco TAC for analysis and corrective action. Refer to the [“Obtaining Technical Assistance”](#) section on page xxxviii for detailed instructions on contacting Cisco TAC and opening a service request.

## Media Gateway or Termination are Found Administratively Out of Service - Signaling (68)

The Media Gateway or Termination are Found Administratively Out of Service alarm (major) indicates that the specified media gateway is going out-of-service due to being powered down, the MGCP application going faulty, or a hardware failure has occurred. The primary causes of the alarm are that the specified media gateway is going out-of-service due to being powered down, the MGCP application going faulty, or a hardware failure has occurred. To correct the primary cause of the alarm, cycle the power on the specified media gateway. For additional troubleshooting information, refer to [Appendix A, “System Usage of MGW Keepalive Parameters, Release 4.4.x.”](#)

## Call Agent and Feature Server Communication Message Timeout - Signaling (69)

The Call Agent and Feature Server Communication Message Timeout alarm (critical) indicates that a CA and FS communications message timed out. The primary cause of the alarm is that CA to FS communication has failed due to wrong system configuration; -OR- CA or FS is down. To correct the primary cause of the alarm, check the configuration related to the CA to FS communication. Also, check the FS table entries and the CA entry.

## Signaling System 7 Stack not Ready - Signaling (75)

The Signaling System 7 Stack not Ready alarm (critical) indicates that the SS7 stack is not ready. The primary cause of the alarm is that the SS7 stack is not configured properly. To correct the primary cause of the alarm, check SS7 stack configuration. The secondary cause of the alarm is that the SS7 stack is not ready. To correct the secondary cause of the alarm, check the SS7 stack status. Do a platform “**start -i omni**” command to bring up the SS7 stack.

## Integrated Services Digital Network Single D-channel Down for Non-Facility Associated Signaling - Signaling (78)

The Integrated Services Digital Network Single D-channel Down for Non-Facility Associated Signaling alarm (minor) indicates that one of the ISDN D-channels in the PRI is down. The primary cause of the alarm is that one of the ISDN D-channels in PRI is down. To correct the primary cause of the alarm, check the gateway power and the gateway connection to the PBX.

## Media Gateway Unreachable - Signaling (79)

The Media Gateway Unreachable alarm (major) indicates that the media gateway is unreachable. The primary cause of the alarm is that a MGCP signaling inter-operational error has occurred. To correct the primary cause of the alarm, refer to [Appendix A, “System Usage of MGW Keepalive Parameters, Release 4.4.x”](#) or contact Cisco TAC. Refer to the “[Obtaining Technical Assistance](#)” section on [page xxxviii](#) for detailed instructions on contacting Cisco TAC and opening a service request.

## Out of Bounds, Memory/Socket Error - Signaling (80)

The Out of Bounds, Memory/Socket Error alarm (critical) indicates that a memory socket out of bounds error has occurred. The primary cause of the alarm is that the system is out of heap memory. To correct the primary cause of the alarm, contact Cisco TAC and increase RAM memory. Refer to the [“Obtaining Technical Assistance” section on page xxxviii](#) for detailed instructions on contacting Cisco TAC and opening a service request. The secondary cause of the alarm is that the system is out of IPC pool memory. To correct the secondary cause of the alarm, resize the IPC pool size in Platform Configuration file. The tertiary cause of the alarm is that a socket error has occurred. An inappropriate or already bound socket may be in use. To correct the tertiary cause of the alarm, check the UDP port supplied with the MGA command-line for validity and prior use.

## Insufficient Heap Memory - Signaling (81) (H.323)

The Insufficient Heap Memory alarm (critical) indicates that there is insufficient heap memory. The primary cause of the alarm is that the H323 signaling adapter was unable to allocate memory from the system. To correct the primary cause of the alarm, contact Cisco TAC for assistance. Refer to the [“Obtaining Technical Assistance” section on page xxxviii](#) for detailed instructions on contacting Cisco TAC and opening a service request.

## Insufficient Shared Memory Pools - Signaling (82) (H.323)

The Insufficient Shared Memory Pools alarm (critical) indicates that there is insufficient shared memory pools. The primary cause of the alarm is that the H323 signaling adapter was unable to allocate storage. To correct the primary cause of the alarm, contact Cisco TAC for corrective action. Refer to the [“Obtaining Technical Assistance” section on page xxxviii](#) for detailed instructions on contacting Cisco TAC and opening a service request.

## Error While Binding to Socket - Signaling (83)

The Error While Binding to Socket alarm (critical) indicates that an error occurred while binding to the socket. To correct the primary cause of the alarm, contact Cisco TAC for corrective action. Refer to the [“Obtaining Technical Assistance” section on page xxxviii](#) for detailed instructions on contacting Cisco TAC and opening a service request.

## Reached Maximum Socket Limit - Signaling (84) (H.323)

The Reached Maximum Socket Limit alarm (critical) indicates that the Cisco BTS 10200 Softswitch system has reached the maximum socket limit. The primary cause of the alarm is that the configuration setting of an H3A parameter in the platform.cfg file is wrong. To correct the primary cause of the alarm, reconfigure the platform.cfg file and restart the H3A process.

## Initialization Failure - Signaling (85)

The Initialization Failure alarm (critical) indicates that the Cisco BTS 10200 Softswitch system failed to initialize. The primary cause of the alarm is that a process initialization failure has occurred. To correct the primary cause of the alarm, check “Reason” dataword for the failure cause and take action accordingly.

## Remote H323 Gateway is not Reachable - Signaling (86) (H.323)

The Remote H323 Gateway is not Reachable alarm (major) indicates that the remote H323 gateway is not reachable. The primary cause of the alarm is that a loss of communication with a remote gateway has occurred. To correct the primary cause of the alarm, perform the standard connectivity tests - both the physical checks and the IP tests. Also, ensure that the gateway is not out of service.

## H323 Message Parsing Error - Signaling (87) (H.323)

The H323 Message Parsing Error alarm (major) indicates that a H323 message parsing error has occurred. The primary cause of the alarm is that the system was unable to successfully parse an incoming H323 message. This alarm is a result of either a software bug or bad message being received - a message with a valid message type but an invalid field within the message. To correct the primary cause of the alarm, snoop the message from the endpoint and verify its content or contact Cisco TAC. Refer to the [“Obtaining Technical Assistance” section on page xxxviii](#) for detailed instructions on contacting Cisco TAC and opening a service request.

## H323 Message Encoding Error - Signaling (88) (H.323)

The H323 Message Encoding Error alarm (major) indicates that a H323 message encoding error has occurred. The primary cause of the alarm is that the system was unable to encode an H323 message for sending. The alarm is indicative a software bug. To correct the primary cause of the alarm, contact Cisco TAC. Refer to the [“Obtaining Technical Assistance” section on page xxxviii](#) for detailed instructions on contacting Cisco TAC and opening a service request.

## Gatekeeper not Available/Reachable - Signaling (89)

The Gatekeeper not Available/Reachable alarm (major) indicates that the gatekeeper is not available or the gatekeeper is not reachable. The primary cause of the alarm is that the gatekeeper is not available or is unreachable. To correct the primary cause of the alarm, check the network connectivity. Check to ensure the GK is reachable by trying to ping the GK IP address. If reachable, then check to ensure that the GK is configured up.

## Alternate Gatekeeper is not Responding - Signaling (90)

The Alternate Gatekeeper is not Responding alarm (major) indicates that the alternate gatekeeper is not responding. The primary cause of the alarm is that the alternate gatekeeper is not responding. To correct the primary cause of the alarm, check network connectivity. Check to ensure the alternate GK is reachable by trying to ping the alternate GK IP address. If reachable, then check to ensure that the alternate GK is configured up.

## Endpoint Security Violation - Signaling (91) (H.323)

The Endpoint Security Violation alarm (major) indicates that an H323 security violation has occurred. The primary cause of the alarm is that an H323 security violation has occurred. To correct the primary cause of the alarm, check to make sure the password selections on the Cisco BTS 10200 Softswitch and the gatekeeper are correct. The secondary cause of the alarm is that the H323GW table may not be provisioned properly or there is a time synchronization problem between the Cisco BTS 10200 Softswitch and/or the gatekeeper and the NTP server. To correct the secondary cause of the alarm, ensure that both the Cisco BTS 10200 Softswitch and the gatekeeper are pointing to the same NTP server.

## Invalid Call Identifier - Signaling (92)

The Invalid Call Identifier alarm (minor) indicates that the Call ID was invalid or changed mid-call. The primary cause of the alarm is that the Call ID was invalid or changed mid-call. The alarm indicates that a software problem has occurred on the Cisco BTS 10200 Softswitch or on the endpoint. To correct the primary cause of the alarm, contact Cisco TAC. Refer to the [“Obtaining Technical Assistance” section on page xxxviii](#) for detailed instructions on contacting Cisco TAC and opening a service request.

## Invalid Call Reference Value - Signaling (93)

The Invalid Call Reference Value alarm (minor) indicates that the Call ID was invalid or changed mid-call. The primary cause of the alarm is that the Call ID was invalid or changed mid-call. The alarm indicates that a software problem has occurred on the Cisco BTS 10200 Softswitch or on the endpoint. To correct the primary cause of the alarm, contact Cisco TAC. Refer to the [“Obtaining Technical Assistance” section on page xxxviii](#) for detailed instructions on contacting Cisco TAC and opening a service request.

## Invalid Conference Identifier - Signaling (94)

The Invalid Conference Identifier alarm (minor) indicates that the Call ID was invalid or changed mid-call. The primary cause of the alarm is that the Call ID was invalid or changed mid-call. The alarm indicates that a software problem has occurred on the Cisco BTS 10200 Softswitch or on the endpoint. To correct the primary cause of the alarm, contact Cisco TAC. Refer to the [“Obtaining Technical Assistance” section on page xxxviii](#) for detailed instructions on contacting Cisco TAC and opening a service request.

## Invalid Message from the Network - Signaling (95)

The Invalid Message from the Network alarm (minor) indicates that an unsupported or invalid message type was received from network. The primary cause of the alarm is that an unsupported or invalid message type was received from the network. To correct the primary cause of the alarm, contact Cisco TAC. Refer to the [“Obtaining Technical Assistance” section on page xxxviii](#) for detailed instructions on contacting Cisco TAC and opening a service request.

## Internal Call Processing Error - Signaling (96)

The Internal Call Processing Error alarm (minor) indicates that an internal call processing error has occurred. The primary cause of the alarm is that a software error has occurred. To correct the primary cause of the alarm, contact Cisco TAC. Refer to the [“Obtaining Technical Assistance” section on page xxxviii](#) for detailed instructions on contacting Cisco TAC and opening a service request.

## Insufficient Information to Complete Call - Signaling (97)

The Insufficient Information to Complete Call alarm (minor) indicates that there was insufficient information to complete a call. The primary cause of the alarm is that there was not enough initial call setup information received to establish the call. To correct the primary cause of the alarm, contact Cisco TAC. Refer to the [“Obtaining Technical Assistance” section on page xxxviii](#) for detailed instructions on contacting Cisco TAC and opening a service request.

## H323 Protocol Inconsistencies - Signaling (98) (H.323)

The H323 Protocol Inconsistencies alarm (minor) indicates that the H323 endpoint and Cisco BTS 10200 Softswitch are running different protocol versions. The primary cause of the alarm is that the H323 endpoint and the Cisco BTS 10200 Softswitch are running different protocol versions. This is only an issue where the endpoint is running a higher version of the H323 protocol than the Cisco BTS 10200 Softswitch. To correct the primary cause of the alarm, contact Cisco TAC. Refer to the [“Obtaining Technical Assistance” section on page xxxviii](#) for detailed instructions on contacting Cisco TAC and opening a service request.

## Abnormal Call Clearing - Signaling (99)

The Abnormal Call Clearing alarm (minor) indicates that an unsupported or invalid message type was received from network. The primary cause of the alarm is that an unsupported or an invalid message type was received from network. To correct the primary cause of the alarm, contact Cisco TAC. Refer to the [“Obtaining Technical Assistance” section on page xxxviii](#) for detailed instructions on contacting Cisco TAC and opening a service request.



## Codec Negotiation Failed - Signaling (100)

The Codec Negotiation Failed alarm (minor) indicates that the codec negotiation has failed. The primary cause of the alarm is that the codec negotiation failed. To correct the primary cause of the alarm, find a compatible set of codec settings for both sides, re-provision the endpoints of the call and try the call again.

## Per Call Security Violation - Signaling (101)

The Per Call Security Violation alarm (minor) indicates that a call security violation has occurred. This is a future trap definition - it will not be issued in the 3.x release series.

## H323 Network Congested - Signaling (102) (H.323)

The H323 Network Congested alarm indicates (minor) that the H323 application process has depleted its resources and no more calls can be completed. The primary cause of this alarm is that the H323 application processes has depleted its resources and no more calls can be completed. The high water mark has been reached and all new call requests are rejected until the low water mark is reached. To correct the primary cause of the alarm, re-provision the water marks or check the network for overload. Also verify that alternate routes have been provisioned on the Cisco BTS 10200 Softswitch.

## Aggregation Connection Down - Signaling (103)

The Aggregation Connection Down alarm (major) indicates that the AGGR TCP connection is down. The primary cause of the alarm is that the TCP connection is down. To correct the primary cause of the alarm, check the associated cabling and perform PINGs to test the connectivity.

## Enhanced Subscriber Authentication Cisco BTS 10200 Softswitch Delivery Function Connection Down - Signaling (106)

The Enhanced Subscriber Authentication Cisco BTS 10200 Softswitch Delivery Function Connection Down alarm (minor) indicates that the ESA Cisco BTS 10200 Softswitch DF connection is down. The primary cause of the alarm is that the DF server is not responding. To correct the primary cause of the alarm, check the encryption key or the IP connectivity to the DF.

## Logical Internet Protocol Addresses not Mapped Correctly - Signaling (107)

The Logical Internet Protocol Addresses not Mapped Correctly alarm (critical) indicates that the logical IP addresses are not mapped correctly. The primary cause of the alarm is that the contact name in the configuration file is not configured in the DNS. To correct the primary cause of the alarm, verify that the name in the DNS matches the name in the platform.cfg and optical.cfg files. The secondary cause of the alarm is the contact could not be resolved to an IP address on the host. To correct the secondary cause of the alarm, verify that the DNS resolves to the IP addresses reserved for process on the Cisco BTS 10200 Softswitch. The tertiary cause of the alarm is that the IP address manager is not running. To correct the tertiary cause of the alarm, verify that the IPM process is running and check for alarms from IPM. The subsequent cause of the alarm is mis-configuration during installation or manual changes made after installation. To correct the subsequent cause of the alarm, contact Cisco TAC for support. Refer to the [“Obtaining Technical Assistance” section on page xxxviii](#) for detailed instructions on contacting Cisco TAC and opening a service request.

## Current SIA Configuration only Valid for Simplex Systems - Signaling (108)

The Current SIA Configuration only Valid for Simplex Systems alarm (major) indicates that the Cisco BTS 10200 Softswitch system can only operate in the simplex mode. The primary cause of the alarm is that the SIA host and contact parameters are the same in platform.cfg file. If this is a duplex installation, regardless of current operational state, contact Cisco TAC. The secondary cause of the alarm is that the SIA is configured for use on a simplex system. If this is a simplex installation only, this alarm can be turned off. Refer to the [“Obtaining Technical Assistance” section on page xxxviii](#) for detailed instructions on contacting Cisco TAC and opening a service request.

## Stream Control Transmission Protocol Association Failure - Signaling (109)

The Stream Control Transmission Protocol Association Failure alarm (major) indicates that the SCTP association failed. This alarm indicates that the Cisco BTS 10200 Softswitch is unable to communicate with an SGP at the SCTP protocol level. The problem may be at the M3UA or SUA layer. The primary cause of the alarm is that the Ethernet cables on the SGP are unplugged or severed. To correct the primary cause of the alarm, plug the Ethernet cables in or fix the severed connection. The secondary cause of the alarm is that the SGP is not operational. To correct the secondary cause of the alarm, check the SGP alarms to determine why it is not operating properly. To troubleshoot the M3UA or the SUA layers, use the following procedures.

### Message Transfer Part 3 User Adapter Troubleshooting Procedure

Use the following steps to determine the source of the problem at the M3UA layer:

**Step 1** Determine if the administrative state of the SCTP is correct.

- a. Type the following command at the Cisco BTS 10200 Softswitch CLI prompt:

```
status sctp-assoc id=<sctp-assoc-name>
```

If the response displays ADMIN STATE ->ADMIN\_OOS, the SCTP association has been taken administratively out of service and needs to be put back in service.

- b. Enter the following command to put the SCTP association in service:

```
control sctp-assoc id=<sctp-assoc-name>; mode=forced; target-state=INS;
```

- c. If the administrative state is ADMIN\_INS, determine if the association has been taken out of service on the ITP. Log on to the ITP. If you are unable to log on to the ITP, proceed to Step 2.
- d. If you are able to log on to the ITP, check the state of the associated application service provider (ASP) by entering the following command:

```
show cs7 asp
```

The following is an example of the output:

| ASP Name | AS Name  | State    | Type | Rmt Port | Remote IP Addr | SCTP  |
|----------|----------|----------|------|----------|----------------|-------|
| -----    | -----    | -----    | ---- | -----    | -----          | ----- |
| hrn11asp | hrn11bts | shutdown | M3UA | 11146    | 10.0.5.13      |       |

- e. If the state of the ASP indicates shutdown, someone has administratively taken the association out of service. Refer to the *Cisco ITP User's Guide*, at the following universal resource locator (URL), to put the ASP (SCTP association) back in service:

<http://www.cisco.com/univercd/cc/td/doc/product/wireless/moblwrls/itp/23sw/index.htm>

- f. If the state is down proceed to Step 2.
- g. If the state of the ASP is inactive, the ASP is probably on the standby Cisco BTS 10200 Softswitch. If the ASP on the active Cisco BTS 10200 Softswitch is inactive, proceed to Step 7.

**Step 2** Determine if the problem is an IP address or port configuration mismatch between the ITP and the Cisco BTS 10200 Softswitch.

- a. Determine the Cisco BTS 10200 Softswitch configured values for the Cisco BTS 10200 Softswitch IP addresses and port. Look for the DNS name and port number that are configured for the SGA process in /opt/OptiCall/CA146/bin/platform.cfg. Go to the specified directory and enter:

```
cat platform.cfg | grep mdl
```

The output will look similar to the following:

```
Args=-t 1 -h mgcp-HRN11CA.hrndevtest.cisco.com -p 11146 -mdldir. /mdl -mdltracedir
../mdltrace -mdltestmode 0 -mdlloadmdo 0 -mdltriggertimer 200 -mdlgarbage timer 5146
-resetcics 1 -fcmtimer 900 -fcmparalleljobs 4
```

- The local IP port number is shown directly after the -p option.
- The local IP addresses that are used by the Cisco BTS 10200 Softswitch are derived from the DNS name, which is given directly after the -h option. At the Cisco BTS 10200 Softswitch UNIX prompt, enter:

```
NSlookup <DNS name>
```

The output will look similar to the following:

```
Server: hrnbtsjs-1.cisco.com
Address: 10.82.70.199
Name: mgcp-HRN11CA.hrndevtest.cisco.com
Addresses: 10.0.5.136, 10.128.1.147
```

The Cisco BTS 10200 Softswitch configured local IP addresses are given in the Addresses: line.

- b. Determine the ITP configured values of the ITP Cisco BTS 10200 Softswitch IP addresses and port.

- Log on to the ITP and get into enable mode.
- Enter the following command:

```
show run
```

- Hit enter until the ASP configurations are displayed. A section similar to the following will appear which shows you the ITP configured values for the Cisco BTS 10200 Softswitch IP addresses of the SCTP association:

```
cs7 asp hrn11asp 11146 2905 m3ua
remote-IP 10.0.5.136
remote-IP 10.128.1.147
```

The number after the ASP name “hrn11asp” is the port number that the ITP has configured for the Cisco BTS 10200 Softswitch side of the SCTP association. The two remote-IP addresses are the addresses that the ITP has configured for the Cisco BTS 10200 Softswitch side of the SCTP association. Make sure all of these values match the values found in Step 2A.

- c. Determine the Cisco BTS 10200 Softswitch configured values for the ITP IP addresses and port

On the Cisco BTS 10200 Softswitch EMS CLI console, type the following:

```
CLI> show sctp-assoc id=<SCTP assoc id>
```

An example of the output will show the IP addresses and port as follows:

```
REMOTE_PORT=2905
REMOTE_TSAP_ADDR1=10.0.1.54
REMOTE_TSAP_ADDR2=10.128.1.239
```

- d. Determine the ITP configured values of the ITP Cisco BTS 10200 Softswitch IP addresses and port
  - Logon to the ITP and get into enable mode.
  - Enter **sho run**.
  - Hit enter until the m3ua (or sua) configuration is displayed. In our example, we are considering the SCTP association connection between the Cisco BTS 10200 Softswitch and the ITP, so we will look at the ITP m3ua configuration. An example of this is as follows:
 

```
cs7 m3ua 2905
local-IP 10.0.1.54
local-IP 10.128.1.239
```
  - Make sure that the IP addresses and port number are the same values as found in step 2C.

**Step 3** Determine if all Ethernet connections on the Cisco BTS 10200 Softswitch have been disconnected or if communication has been lost to the IP router. In the platform.log, look for the following ERROR message:

“All the IP interfaces are faulty!!”

If this message is found, the Ethernet connections of the Cisco BTS 10200 Softswitch have been pulled or cut. If this message is not found, proceed to Step 4.

**Step 4** Determine if the problem is an IP routing issue.

- a. Determine what has been provisioned in the Cisco BTS 10200 Softswitch for the destination IP interfaces of the SCTP association by typing the following command:

```
show sctp-association id=<sctp-association-id>
```

Information similar to the following will appear and display the destination IP addresses:

```
REMOTE_TSAP_ADDR1=10.0.1.54
REMOTE_TSAP_ADDR2=10.128.1.239
```

- b. Ping each of the destination IP addresses. If one of the addresses does not respond to the ping, there is an IP routing problem that has disabled SCTP communication. Contact the Cisco TAC for assistance. If the ping commands are successful, proceed to Step 5.

**Step 5** Determine if the Cisco BTS 10200 Softswitch is reachable from the ITP.

- a. Log on to the ITP and get into enable mode.
- b. Find the Cisco BTS 10200 Softswitch SCTP association endpoint IP addresses by typing the following command:

```
show run
```

- c. Hit enter until the ASP configuration is displayed. A section similar to the following will display the Cisco BTS 10200 Softswitch IP addresses of the SCTP association:

```
cs7 asp hrn11asp 11146 2905 m3ua
remote-IP 10.0.5.136
remote-IP 10.128.1.147
```

- d. Ping each of the IP addresses. If you do not receive a response to the ping command for at least one of the Cisco BTS 10200 Softswitch IP endpoint addresses, there is an IP routing problem that is causing the SCTP association to be down. Contact the Cisco TAC for assistance. Otherwise, proceed to Step 6.

**Step 6** Bounce the SCTP association (take it administratively out of service and then put it in service)

- a. At the Cisco BTS 10200 Softswitch CLI prompt, enter the following commands:

```
control sctp-assoc id=<sctp-assoc-name>; mode=forced; target-state=OOS;
control sctp-assoc id=<sctp-assoc-name>; mode=forced; target-state=INS;
```

- b. Check if the SCTP association has come back in service by entering the following:

```
status sctp-assoc id=<sctp-assoc-name>;
```

The output will either show OPER STATE -> SCTP-ASSOC out of service or OPER STATE -> SCTP-ASSOC in service.

If the OPER STATE still shows that the SCTP association is out-of-service, proceed to Step 7.

**Step 7** Bounce the SCTP association from the ITP side by performing the following steps:

- a. Log on to the ITP and get into enable mode.  
b. Get into configure mode by typing configure terminal.  
c. Type the following commands to bounce the SCTP association back in service:

```
va-2651-82(config)#cs7 asp hrn11asp
va-2651-82(config-cs7-asp)#shut
va-2651-82(config-cs7-asp)#no shut
va-2651-82(config-cs7-asp)#end
```

- d. Determine if the SCTP association has come back in service by typing the following Cisco BTS 10200 Softswitch CLI command:

```
status sctp-assoc id=<sctp-assoc-name>;
```

The output will display either OPER STATE -> SCTP-ASSOC out of service or OPER STATE -> SCTP-ASSOC in service.

If the OPER STATE still shows that the SCTP association is out-of-service, there is probably an SCTP communication issue that must be debugged at the SCTP protocol level. Contact the Cisco TAC for assistance.

## Signaling Connection Control Part User Adapter Troubleshooting Procedures

Refer to [Chapter 13, “Network Troubleshooting”](#) to determine the source of the problem at the SUA layer.

## Signaling Gateway Group Is Out-of-Service - Signaling (110)

The Signaling Gateway Group is Out-of-Service alarm (major) indicates that the signaling gateway group is out-of-service. The primary cause of the alarm is that all the SCTP associations between the CA and the SGs are out-of-service. To correct the primary cause of the alarms, make sure that all Ethernet connections on the CA and SGs are plugged in. Also make sure all associated IP routers are operational. The secondary cause of the alarm is that the M3UA layer is down between the CA and SGs. To correct the secondary cause of the alarm, use a snoop application to determine why the M3UA layer is down.

This alarm indicates that after communication to the SG group was established, it was lost. This indicates that communication to associated SGs is down, which also indicates that communication to all SGPs is down. See the [“Signaling Gateway Failure - Signaling \(113\)”](#) section on page 10-126 to determine why the associated SGs are down.

## Stream Control Transmission Protocol Association Degraded (One of Two Internet Protocol Connections Down) - Signaling (111)

The Stream Control Transmission Protocol Association Degraded (One of Two Internet Protocol Connections Down) alarm (major) indicates that the SCTP association is degraded. The primary cause of the alarm is that a single Ethernet connection on CA or SGP is unplugged or severed. To correct the primary cause of the alarm, plug in all Ethernet connections or repair if severed. The secondary cause of the alarm is a SCTP communication problem - or protocol timeout. To correct the secondary cause of the alarm, use a snoop application to determine why the SCTP association is degraded.

### Message Transfer Part 3 User Adapter Troubleshooting Procedure

This alarm indicates that one of the two sides of the multi-homed SCTP connection is down. Communication still exists if the other side of the multi-homed connection is up. Refer to the [“Stream Control Transmission Protocol Association Degraded \(One of Two Internet Protocol Connections Down\) - Signaling \(111\)”](#) section on page 10-125, or contact the Cisco TAC for assistance in resolving this issue. Refer to the [“Obtaining Technical Assistance”](#) section on page xxxviii for detailed instructions on contacting Cisco TAC and opening a service request.

### Signaling Connection Control Part User Adapter Troubleshooting Procedure

This is either an IP routing problem or an ITP Ethernet port hardware failure. Change the hardware immediately, if it is a hardware failure, to prevent dual outage of the ITP's IP communication.

## Stream Control Transmission Protocol Association Configuration Error - Signaling (112)

The Stream Control Transmission Protocol Association Configuration Error alarm (minor) indicates that a SCTP association configuration error has occurred. The primary cause of the alarm is that the destination IP address is invalid. To correct the primary cause of the alarm, input a new destination IP address, see the log for additional details. The secondary cause of the alarm is that the local IP address is invalid. To correct the secondary cause of the alarm, input new local IP address information. The tertiary cause of the alarm is that the IP Routing Table is not configured properly. To correct the tertiary cause of the alarm, have the system administrator configure IP routing table.

### Message Transfer Part 3 User Adapter Troubleshooting Procedure

This alarm indicates that there is a provisioning error keeping the Cisco BTS 10200 Softswitch from properly configuring the SCTP association. Perform the following steps to resolve the problem:

- 
- Step 1** To get more information about this alarm, look at the platform.log for error messages containing the string “Multipurpose Internet Mail (MIM) configuration (CFG).”
  - Step 2** Perform Step 2 of the [“Stream Control Transmission Protocol Association Degraded \(One of Two Internet Protocol Connections Down\) - Signaling \(111\)”](#) section on page 10-125 to verify that your IP addresses and ports are properly configured on the Cisco BTS 10200 Softswitch.
  - Step 3** Contact the Cisco TAC for assistance in resolving this issue. Refer to the [“Obtaining Technical Assistance”](#) section on page xxxviii for detailed instructions on contacting Cisco TAC and opening a service request.
- 

### Signaling Connection Control Part User Adapter Troubleshooting Procedure

Refer to [Chapter 13, “Network Troubleshooting”](#) to verify that the IP addresses and ports are properly configured on the Cisco BTS 10200 Softswitch.

## Signaling Gateway Failure - Signaling (113)

The Signaling Gateway Failure alarm (major) indicates that all associated signaling gateway processes are out-of-service. The primary cause of the alarm is that all associated Signaling Gateway Processes are out-of-service. To correct the primary cause of the alarm, determine why each associated Signaling Gateway Process is out-of-service (see SGP alarm definition).

This alarm indicates that communication at the M3UA layer to an SG has failed. M3UA communications at all SGPs that make up the SG are unavailable. See the [“Stream Control Transmission Protocol Association Degraded \(One of Two Internet Protocol Connections Down\) - Signaling \(111\)”](#) section on page 10-125 to determine why the associated SGPs are down.



## Signaling Gateway Process Is Out-of-Service - Signaling (114)

The Signaling Gateway Process is Out-of-Service alarm (major) indicates that all SCTP associations between the SGP and the CA are out-of-service. The primary cause of the alarm is that all SCTP associations between the SGP and the CA are out-of-service. To correct the primary cause of the alarm, see the SCTP Association Alarm definition to determine how to rectify the problem. The secondary cause of the alarm is that the M3UA layer is down between the CA and the SGP. To correct the secondary cause of the alarm, use a snoop utility to determine why M3UA layer is down. Also see the log for additional information.

This alarm indicates that communication at the M3UA layer to an SGP has failed. In the majority of cases, there will also be a related SCTP Association Failure alarm. If this is the case, proceed to the [“Stream Control Transmission Protocol Association Degraded \(One of Two Internet Protocol Connections Down\) - Signaling \(111\)”](#) section on page 10-125. Otherwise, the problem is at the M3UA layer. Call the Cisco TAC for assistance. Refer to the [“Obtaining Technical Assistance”](#) section on page xxxviii for detailed instructions on contacting Cisco TAC and opening a service request.

## Destination Point Code User Part Unavailable - Signaling (116)

The Destination Point Code User Part Unavailable alarm (major) indicates that a layer 4 user part, such as ISUP, is unavailable at the DPC in the SS7 network. The primary cause of the alarm is that the SGP sent a DUPU M3UA message to the CA indicating that an user part is unavailable on at a DPC. To correct the primary cause of the alarm, contact the SS7 network administrator to report the user part unavailable problem related to the DPC so communication can be restored.

## Circuit Validation Test Message Received for an Unequipped Circuit Identification Code - Signaling (117)

The Circuit Validation Test Message Received for an Unequipped Circuit Identification Code alarm (minor) indicates that a CVT message was received for an unequipped CIC. The primary cause of the alarm is that the CIC is not provisioned. To correct the primary cause of the alarm, provision the CIC.

## Circuit Verification Response Received with Failed Indication - Signaling (118)

The Circuit Verification Response Received with Failed Indication alarm (minor) indicates that a CVR message was received with a failure indication. The primary cause of the alarm is that a CIC mismatch has occurred. To correct the primary cause of the alarm, perform an internal test such as checking that the CIC is assigned to a circuit between the sending and the receiving switch.

## Signaling System 7 Adapter Process Faulty - Signaling (119)

The Signaling System 7 Adapter Process Faulty alarm (critical) indicates that a S7A process is faulty. The primary cause of the alarm is that an OMNI or a S7A exception has occurred. To correct the primary cause of the alarm, check OMNI process. The S7A process will restart itself if the S7A maximum restart threshold has not been exceeded.

## Signaling System 7 Module/Signaling System 7 Adapter Faulty - Signaling (120)

The Signaling System 7 Module/Signaling System 7 Adapter Faulty alarm (critical) indicates that the S7M/S7A processes are faulty. The primary cause of the alarm is that an OMNI failure has occurred. To correct the primary cause of the alarm, check the OMNI status. An automatic failover will occur in a duplex configuration.

## Message Transfer Part 3 User Adapter Cannot Go Standby - Signaling (121)

The Message Transfer Part 3 User Adapter Cannot Go Standby alarm (major) indicates that the M3UA process cannot go into standby mode. The primary cause of the alarm is that no INACTIVE ACK messages are being received from any Signaling Gateway. The SG or SCTP associations are probably down. To correct the primary cause of the alarm, investigate other alarms to see if SGs are down or if SCTP associations are down. Take corrective action according to those alarms.

This alarm is raised at initial startup or during failover by the Cisco BTS 10200 Softswitch node that is trying to go into platform Standby mode. See the [“Stream Control Transmission Protocol Association Degraded \(One of Two Internet Protocol Connections Down\) - Signaling \(111\)”](#) section on page 10-125 to determine why the Cisco BTS 10200 Softswitch is unable to communicate with any of the SGs at the M3UA layer. See the [“Verify the Stream Control Transmission Protocol Association Status”](#) section on page 13-2 to determine why the Cisco BTS 10200 Softswitch is unable to communicate with any of the ITPs at the SUA layer.

## Message Transfer Part 3 User Adapter Cannot Go Active - Signaling (122)

The Message Transfer Part 3 User Adapter Cannot Go Active alarm (major) indicates that the M3UA process cannot go into active mode. The primary cause of the alarm is that no ACTIVE ACK messages are being received from any Signaling Gateway. The SG or SCTP associations are probably down. To correct the primary cause of the alarm, investigate other alarms to see if SGs are down or if the SCTP associations are down. Take corrective action according to those alarms.

This alarm is raised at initial startup or during failover by the Cisco BTS 10200 Softswitch node that is trying to go into platform Active mode. It occurs when this Cisco BTS 10200 Softswitch node is unable to communicate properly with any SGs to tell them that all active call traffic should be routing towards the Cisco BTS 10200 Softswitch. See the [“Stream Control Transmission Protocol Association Degraded \(One of Two Internet Protocol Connections Down\) - Signaling \(111\)”](#) section on page 10-125 to determine why the Cisco BTS 10200 Softswitch is unable to communicate with any of the ITPs at the M3UA layer. Refer to the [“Verify the Stream Control Transmission Protocol Association Status”](#) section on page 13-2 to determine why the Cisco BTS 10200 Softswitch is unable to communicate with any of the ITPs at the SUA layer.

## Remote Subsystem is Out Of Service - Signaling (124)

The Remote Subsystem is out of Service alarm (minor) indicates that the remote subsystem is out-of-service. The primary cause of the alarm is that the link lost connection or the remote subsystem is out-of-service. This alarm indicates the remote subsystem is out-of-service. To correct the primary cause of the alarm, contact your service control point (SCP) service provider for assistance.

## Signaling Connection Control Part Routing Error - Signaling (125)

The Signaling Connection Control Part Routing Error alarm (major) indicates that the SCCP route was invalid or not available. The primary cause of the alarm is that the SCCP route is invalid or is not available. To correct the primary cause of the alarm, provision the right SCCP route.

## Signaling Connection Control Part Binding Failure - Signaling (126)

The Signaling Connection Control Part Binding Failure alarm (major) indicates that the SCCP binding failed. The primary cause of the SCCP Binding Failure alarm is that the Trillium stack binding failed. To correct the primary cause of the alarm, re-initialize the TSA process or remove the subsystem from the EMS table and add it again.

## Transaction Capabilities Application Part Binding Failure - Signaling (127)

The Transaction Capabilities Application Part Binding Failure alarm (major) indicates that the TCAP binding failed. This alarm is raised when the TCAP layer does not have enough service access point (SAP) to bind for the subsystem. Currently only 16 subsystems are allowed on the same platform. Check the Subsystem table to see if you have more than 16 subsystems on the same platform, Feature Server for POTS, Tandem, and Centrex services (FSPTC) or Feature Server for AIN services (FSAIN). The primary cause of the TCAP Binding Failure alarm is that the Trillium stack binding failed. To correct the primary cause of the alarm, re-initialize the TSA process or remove the subsystem from the EMS table and add it again.

## Number of Open Session Initiation Protocol Connections is Reaching Engineered Limit - Signaling (138)

The Number of Open Session Initiation Protocol Connections is Reaching Engineered Limit alarm (minor) indicates that the number of open SIP connections is reaching the engineered limit. The primary cause of the event is that the system configuration and traffic load have caused the number of open connections to approach the engineered limit. To correct the primary cause of the event, increase the engineered limit to allow for more open connections. Contact Cisco TAC for assistance in increasing in the limit. Refer to the [“Obtaining Technical Assistance”](#) section on page xxxviii for detailed instructions on contacting Cisco TAC and opening a service request.

## Session Initiation Protocol Trunk Operationally Out-of-Service - Signaling (142)

The Session Initiation Protocol Trunk Operationally Out-of-Service alarm (critical) indicates that the SIP trunk is operationally out-of-service. The primary cause of the alarm is that the Cisco BTS 10200 Softswitch is unable to communicate with a remote SIP party (Call-Agent or Proxy) over a SIP or SIP-T trunk. To correct the primary cause of the alarm, verify that the DNS resolution exists, if TSAP address of the remote entity is a domain name. Verify the remote entity is reachable by ICMP ping, using the Trunk TSAP address from the alarm event report. If the same alarm is reported on all the softswitch trunk groups, then verify that the network connection is operational. If the ping is not successful, then diagnose the issue that prevents the TSAP address from being reached. Verify the SIP application is running on the remote host and listening on the port specified in the TSAP address.

## **Internet Protocol Interface Link to the Signaling System 7 Signaling Gateway is Down - Signaling (143)**

The Internet Protocol Interface Link to the Signaling System 7 Signaling Gateway is Down alarm (minor) indicates that an IP interface link to the SS7 signaling gateway is down. The primary cause of the alarm is an interface hardware problem. To correct the primary cause of the alarm, check the link interfaces.

## **All Internet Protocol Interface Links to Signaling System 7 Signaling Gateway are Down - Signaling (144)**

The All Internet Protocol Interface Links to Signaling System 7 Signaling Gateway are Down alarm (critical) indicates that all IP interface links to the SS7 signaling gateway are down. The primary cause of the alarm is an interface hardware problem. To correct the primary cause of the alarm, check the link interfaces.

## **One Internet Protocol Interface to Signaling System 7 Signaling Gateway is Down - Signaling (145)**

The One Internet Protocol Interface to Signaling System 7 Signaling Gateway is Down alarm (minor) indicates that one IP interface link to the SS7 signaling gateway is down. The primary cause of the alarm is an interface hardware problem. To correct the primary cause of the alarm, check the link interfaces.

## **Stream Control Transmission Protocol Association Congested - Signaling (150)**

The Stream Control Transmission Protocol Association Congested alarm (minor) indicates that the SCTP association is congested. The primary cause of the alarm is that the network is congested. To correct the primary cause of the alarm, clean off the network congestion caused by routing or switching issues. The secondary cause of the alarm is that the CPU is throttled. To correct the secondary cause of the alarm, upgrade to a more powerful platform or offload some traffic.



# CHAPTER 11

## Statistics Troubleshooting

---

Revised: October 23, 2008, OL-11335-06

### Introduction

This chapter provides the information needed to monitor and troubleshoot Statistics events and alarms. This chapter is divided into the following sections:

- [Statistics Events and Alarms](#) – Provides a brief overview of each Statistics event and alarm.
- [Monitoring Statistics Events](#) – Provides the information needed to monitor and correct Statistics events.
- [Troubleshooting Statistics Alarms](#) – Provides the information needed to troubleshoot and correct Statistics alarms.

# Statistics Events and Alarms

This section provides a brief overview of the Security events and alarms for the Cisco BTS 10200 Softswitch in numerical order. [Table 11-1](#) lists all of the statistics events and alarms by severity.


**Note**

Click the Statistics message number in [Table 11-1](#) to display information about the event or alarm.

**Table 11-1**      *Statistics Events and Alarms by Severity*

| CRITICAL | MAJOR                           | MINOR | WARNING                         | INFO                           |
|----------|---------------------------------|-------|---------------------------------|--------------------------------|
|          | <a href="#">STATISTICS (12)</a> |       | <a href="#">STATISTICS (8)</a>  | <a href="#">STATISTICS (1)</a> |
|          | <a href="#">STATISTICS (13)</a> |       | <a href="#">STATISTICS (9)</a>  | <a href="#">STATISTICS (2)</a> |
|          |                                 |       | <a href="#">STATISTICS (10)</a> | <a href="#">STATISTICS (3)</a> |
|          |                                 |       | <a href="#">STATISTICS (11)</a> | <a href="#">STATISTICS (4)</a> |
|          |                                 |       |                                 | <a href="#">STATISTICS (5)</a> |
|          |                                 |       |                                 | <a href="#">STATISTICS (6)</a> |
|          |                                 |       |                                 | <a href="#">STATISTICS (7)</a> |

## STATISTICS (1)

For additional information, refer to the [“Test Report - Statistics \(1\)”](#) section on page 11-11.

|             |                    |
|-------------|--------------------|
| DESCRIPTION | Test Report        |
| SEVERITY    | Information (INFO) |
| THRESHOLD   | 10000              |
| THROTTLE    | 0                  |

## STATISTICS (2)

For additional information, refer to the [“Call Agent Measurement Collection Started - Statistics \(2\)”](#) section on page 11-11.

|                |                                                                                                    |
|----------------|----------------------------------------------------------------------------------------------------|
| DESCRIPTION    | Call Agent Measurement Collection Started                                                          |
| SEVERITY       | INFO                                                                                               |
| THRESHOLD      | 100                                                                                                |
| THROTTLE       | 0                                                                                                  |
| DATAWORDS      | Start Time - STRING [40]                                                                           |
| PRIMARY CAUSE  | Indicates that the 15-minute traffic measurement collection process has started on the Call Agent. |
| PRIMARY ACTION | No action is necessary.                                                                            |

## STATISTICS (3)

For additional information, refer to the [“Call Agent Measurement Collection Finished - Statistics \(3\)” section on page 11-11.](#)

|                |                                                                                                      |
|----------------|------------------------------------------------------------------------------------------------------|
| DESCRIPTION    | Call Agent Measurement Collection Finished                                                           |
| SEVERITY       | INFO                                                                                                 |
| THRESHOLD      | 100                                                                                                  |
| THROTTLE       | 0                                                                                                    |
| DATAWORDS      | End Time - STRING [40]                                                                               |
| PRIMARY CAUSE  | Indicates that the 15-minute traffic measurement collection process has completed on the Call Agent. |
| PRIMARY ACTION | No action is necessary.                                                                              |

## STATISTICS (4)

For additional information, refer to the [“Plain Old Telephone Service/Centrex/Telecommunications Data Link Monitor Feature Server Measurement Collection Started - Statistics \(4\)” section on page 11-12.](#)

|                |                                                                                                                                                                                     |
|----------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| DESCRIPTION    | Plain Old Telephone Service/Centrex/Telecommunications Data Link Monitor Feature Server Measurement Collection Started (POTS/CTX/TDM Feature Server Measurement Collection Started) |
| SEVERITY       | INFO                                                                                                                                                                                |
| THRESHOLD      | 100                                                                                                                                                                                 |
| THROTTLE       | 0                                                                                                                                                                                   |
| DATAWORDS      | Start Time - STRING [40]                                                                                                                                                            |
| PRIMARY CAUSE  | Indicates that the 15-minute traffic measurement collection process has started on the plain old telephone service (POTS)/Centrex/Tandem Feature Server.                            |
| PRIMARY ACTION | No action is necessary.                                                                                                                                                             |

## STATISTICS (5)

For additional information, refer to the [“Plain Old Telephone Service/Centrex/Telecommunications Data Link Monitor Feature Server Measurement Collection Finished - Statistics \(5\)”](#) section on page 11-12.

|                |                                                                                                                                                                                       |
|----------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| DESCRIPTION    | Plain Old Telephone Service/Centrex/Telecommunications Data Link Monitor Feature Server Measurement Collection Finished (POTS/CTX/TDM Feature Server Measurement Collection Finished) |
| SEVERITY       | INFO                                                                                                                                                                                  |
| THRESHOLD      | 100                                                                                                                                                                                   |
| THROTTLE       | 0                                                                                                                                                                                     |
| DATAWORDS      | End Time - STRING [40]                                                                                                                                                                |
| PRIMARY CAUSE  | Indicates that the 15-minute traffic measurement collection process has finished on the POTS/Centrex/Tandem Feature Server.                                                           |
| PRIMARY ACTION | No action is necessary.                                                                                                                                                               |

## STATISTICS (6)

For additional information, refer to the [“Advanced Intelligent Network Feature Server Measurement Collection Started - Statistics \(6\)”](#) section on page 11-12.

|                |                                                                                                                                           |
|----------------|-------------------------------------------------------------------------------------------------------------------------------------------|
| DESCRIPTION    | Advanced Intelligent Network Feature Server Measurement Collection Started (AIN Feature Server Measurement Collection Started)            |
| SEVERITY       | INFO                                                                                                                                      |
| THRESHOLD      | 100                                                                                                                                       |
| THROTTLE       | 0                                                                                                                                         |
| DATAWORDS      | Start Time - STRING [40]                                                                                                                  |
| PRIMARY CAUSE  | Indicates that the 15-minute traffic measurement collection process has started on the Advanced Intelligent Network (AIN) feature server. |
| PRIMARY ACTION | No action is necessary.                                                                                                                   |



## STATISTICS (7)

For additional information, refer to the [“Advanced Intelligent Network Feature Server Measurement Collection Finished - Statistics \(7\)”](#) section on page 11-12.

|                |                                                                                                                                  |
|----------------|----------------------------------------------------------------------------------------------------------------------------------|
| DESCRIPTION    | Advanced Intelligent Network Feature Server Measurement Collection Finished (AIN Feature Server Measurement Collection Finished) |
| SEVERITY       | INFO                                                                                                                             |
| THRESHOLD      | 100                                                                                                                              |
| THROTTLE       | 0                                                                                                                                |
| DATAWORDS      | End Time - STRING [40]                                                                                                           |
| PRIMARY CAUSE  | Indicates that the 15-minute traffic measurement collection process has completed on the AIN feature server.                     |
| PRIMARY ACTION | No action is necessary.                                                                                                          |

## STATISTICS (8)

To monitor and correct the cause of the event, refer to the [“Message Send Failure - Statistics \(8\)”](#) section on page 11-13.

|                  |                                                                                                                                            |
|------------------|--------------------------------------------------------------------------------------------------------------------------------------------|
| DESCRIPTION      | Message Send Failure                                                                                                                       |
| SEVERITY         | WARNING                                                                                                                                    |
| THRESHOLD        | 100                                                                                                                                        |
| THROTTLE         | 0                                                                                                                                          |
| DATAWORDS        | Originating Process - STRING [40]<br>Traffic Mgr Msg Type - STRING [40]<br>Traffic Agent Msg Ty - STRING [30]                              |
| PRIMARY CAUSE    | Originating process (for Call Agent (CA), Feature Server (FS) or Element Management System (EMS)) is not in active state, or is shut down. |
| PRIMARY ACTION   | Check for other alarms and events generated from this component (CA, FS or EMS).                                                           |
| SECONDARY CAUSE  | Hub is down.                                                                                                                               |
| SECONDARY ACTION | If the originating process is down, try to bring the process back into the normal state.                                                   |
| TERNARY CAUSE    | Platform is currently shutting down a process.                                                                                             |
| TERNARY ACTION   | If the hub process is down, try to bring it into a normal state. (Contact Cisco Technical Assistance Center (TAC).)                        |

Refer to the [“Obtaining Technical Assistance”](#) section on page xxxviii for detailed instructions on contacting Cisco TAC and opening a service request.

## STATISTICS (9)

To monitor and correct the cause of the event, refer to the [“Measurement Table Structured Query Language Read Error - Statistics \(9\)”](#) section on page 11-13.

|                  |                                                                                                                                           |
|------------------|-------------------------------------------------------------------------------------------------------------------------------------------|
| DESCRIPTION      | Measurement Table Structured Query Language Read Error (Measurement Table SQL Read Error)                                                 |
| SEVERITY         | WARNING                                                                                                                                   |
| THRESHOLD        | 100                                                                                                                                       |
| THROTTLE         | 0                                                                                                                                         |
| DATAWORDS        | Measurement Table Na - STRING [40]                                                                                                        |
| PRIMARY CAUSE    | There is no database connection or the connection is faulty.                                                                              |
| PRIMARY ACTION   | Check to see if there are any other events generated that indicate there is a database problem.                                           |
| SECONDARY CAUSE  | Traffic measurement table(s) are corrupted.                                                                                               |
| SECONDARY ACTION | Correct any database-related problems.                                                                                                    |
| TERNARY CAUSE    | Two processors or more are attempting to access the table at the same time.                                                               |
| TERNARY ACTION   | If all of the database-related problems are cleared, and this warning event report still occurs, contact Cisco TAC for technical support. |

Refer to the [“Obtaining Technical Assistance”](#) section on page xxxviii for detailed instructions on contacting Cisco TAC and opening a service request.

## STATISTICS (10)

To monitor and correct the cause of the event, refer to the [“Measurement Table Structured Query Language Write Error - Statistics \(10\)”](#) section on page 11-14.

|                  |                                                                                                                                           |
|------------------|-------------------------------------------------------------------------------------------------------------------------------------------|
| DESCRIPTION      | Measurement Table Structured Query Language Write Error (Measurement Table SQL Write Error)                                               |
| SEVERITY         | WARNING                                                                                                                                   |
| THRESHOLD        | 100                                                                                                                                       |
| THROTTLE         | 0                                                                                                                                         |
| DATAWORDS        | Measurement Table Na - STRING [40]                                                                                                        |
| PRIMARY CAUSE    | There is no database connection or the connection is faulty.                                                                              |
| PRIMARY ACTION   | Check to see if there are any other events generated that indicate there is a database problem.                                           |
| SECONDARY CAUSE  | Traffic measurement table(s) are corrupted.                                                                                               |
| SECONDARY ACTION | Correct any database-related problems.                                                                                                    |
| TERNARY CAUSE    | Two processors or more are attempting to access the table at the same time.                                                               |
| TERNARY ACTION   | If all of the database-related problems are cleared, and this warning event report still occurs, contact Cisco TAC for technical support. |

Refer to the [“Obtaining Technical Assistance”](#) section on page xxxviii for detailed instructions on contacting Cisco TAC and opening a service request.

## STATISTICS (11)

To monitor and correct the cause of the event, refer to the [“Measurement Collection Application Programming Interface Failure - Statistics \(11\)”](#) section on page 11-14.

|                   |                                                                                                                                                                                                          |
|-------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| DESCRIPTION       | Measurement Collection Application Programming Interface Failure (Measurement Collection API Failure)                                                                                                    |
| SEVERITY          | WARNING                                                                                                                                                                                                  |
| THRESHOLD         | 100                                                                                                                                                                                                      |
| THROTTLE          | 0                                                                                                                                                                                                        |
| DATAWORDS         | Message Type - STRING [40]<br>Platform Type - STRING [40]                                                                                                                                                |
| PRIMARY CAUSE     | This report is issued when the traffic measurement subsystem on the call agent or feature server encounters difficulties when it tries to collect measurement values from one of the processes.          |
| PRIMARY ACTION    | Execute a status command for the affected call agent or feature server.                                                                                                                                  |
| SECONDARY CAUSE   | Originating process (for CA, FS or EMS) is not in active state or is shut down.                                                                                                                          |
| SECONDARY ACTION  | If the status report indicates that the originating process is down, try to bring the process back into the normal (In Service) state. If you need assistance in restoring a process, contact Cisco TAC. |
| TERNARY CAUSE     | Platform is currently shutting down the originating process.                                                                                                                                             |
| TERNARY ACTION    | If this event report is being issued every collection period, contact Cisco TAC for assistance.                                                                                                          |
| SUBSEQUENT ACTION | <b>Note</b> Traffic measurements will not be available for the affected call agent or feature server from the measurement period in which this event report was issued.                                  |

Refer to the [“Obtaining Technical Assistance”](#) section on page xxxviii for detailed instructions on contacting Cisco TAC and opening a service request.

## STATISTICS (12)

To troubleshoot and correct the cause of the alarm, refer to the [“Measurement Handshake Error - Schema Inconsistency - Statistics \(12\)”](#) section on page 11-16.

|                  |                                                                         |
|------------------|-------------------------------------------------------------------------|
| DESCRIPTION      | Measurement Handshake Error - Schema Inconsistency                      |
| SEVERITY         | MAJOR                                                                   |
| THRESHOLD        | 5                                                                       |
| THROTTLE         | 0                                                                       |
| DATAWORDS        | Schemas Out of Synchronization - STRING [64]                            |
| PRIMARY CAUSE    | Counters added/deleted from schema in Oracle but not in the call agent. |
| PRIMARY ACTION   | Add/delete the counters on the CA.                                      |
| SECONDARY CAUSE  | Load is installed incorrectly.                                          |
| SECONDARY ACTION | Reinstall the load.                                                     |

## STATISTICS (13)

To troubleshoot and correct the cause of the alarm, refer to the [“Traffic and Measurements Module Application Programming Interface Failure - Statistics \(13\)”](#) section on page 11-16.

|                   |                                                                                             |
|-------------------|---------------------------------------------------------------------------------------------|
| DESCRIPTION       | Traffic and Measurements Module Application Programming Interface Failure (TMM API Failure) |
| SEVERITY          | MAJOR                                                                                       |
| THRESHOLD         | 1                                                                                           |
| THROTTLE          | 10                                                                                          |
| DATAWORDS         | TMM Error - FOUR_BYTES                                                                      |
| PRIMARY CAUSE     | Unable to initialize shared memory.                                                         |
| PRIMARY ACTION    | Reconfigure and restart system.                                                             |
| SECONDARY CAUSE   | Unable to attach to shared memory.                                                          |
| SECONDARY ACTION  | Restart offending process.                                                                  |
| TERNARY CAUSE     | Shared memory table overflow.                                                               |
| TERNARY ACTION    | Reconfigure/restart or fix problematic application.                                         |
| SUBSEQUENT CAUSE  | Shared memory exhaustion.                                                                   |
| SUBSEQUENT ACTION | Reconfigure and restart system.                                                             |

# Monitoring Statistics Events

This section provides the information needed to monitor and correct Statistics events. [Table 11-2](#) lists all Statistics events in numerical order and provides cross reference to each subsection in this section.

**Table 11-2** *Cisco BTS 10200 Softswitch Statistics Events*

| Event Type     | Event Name                                                                                                                                               | Event Severity |
|----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------|----------------|
| STATISTICS(1)  | <a href="#">Test Report - Statistics (1)</a>                                                                                                             | INFO           |
| STATISTICS(2)  | <a href="#">Call Agent Measurement Collection Started - Statistics (2)</a>                                                                               | INFO           |
| STATISTICS(3)  | <a href="#">Call Agent Measurement Collection Finished - Statistics (3)</a>                                                                              | INFO           |
| STATISTICS(4)  | <a href="#">Plain Old Telephone Service/Centrex/Telecommunications Data Link Monitor Feature Server Measurement Collection Started - Statistics (4)</a>  | INFO           |
| STATISTICS(5)  | <a href="#">Plain Old Telephone Service/Centrex/Telecommunications Data Link Monitor Feature Server Measurement Collection Finished - Statistics (5)</a> | INFO           |
| STATISTICS(6)  | <a href="#">Advanced Intelligent Network Feature Server Measurement Collection Started - Statistics (6)</a>                                              | INFO           |
| STATISTICS(7)  | <a href="#">Advanced Intelligent Network Feature Server Measurement Collection Finished - Statistics (7)</a>                                             | INFO           |
| STATISTICS(8)  | <a href="#">Message Send Failure - Statistics (8)</a>                                                                                                    | WARNING        |
| STATISTICS(9)  | <a href="#">Measurement Table Structured Query Language Read Error - Statistics (9)</a>                                                                  | WARNING        |
| STATISTICS(10) | <a href="#">Measurement Table Structured Query Language Write Error - Statistics (10)</a>                                                                | WARNING        |
| STATISTICS(11) | <a href="#">Measurement Collection Application Programming Interface Failure - Statistics (11)</a>                                                       | WARNING        |
| STATISTICS(12) | <a href="#">Measurement Handshake Error - Schema Inconsistency - Statistics (12)</a>                                                                     | MAJOR          |
| STATISTICS(13) | <a href="#">Traffic and Measurements Module Application Programming Interface Failure - Statistics (13)</a>                                              | MAJOR          |

## Test Report - Statistics (1)

The Test Report event is for testing the statistics event category. The event is informational and no further action is required.

## Call Agent Measurement Collection Started - Statistics (2)

The Call Agent Measurement Collection Started event functions as an informational alert that the call agent measurement collection has started. The event is informational and no further action is required.

## Call Agent Measurement Collection Finished - Statistics (3)

The Call Agent Measurement Collection Finished event functions as an informational alert that the call agent measurement collection is finished. The event is informational and no further action is required.

## **Plain Old Telephone Service/Centrex/Telecommunications Data Link Monitor Feature Server Measurement Collection Started - Statistics (4)**

The Plain Old Telephone Service/Centrex/Telecommunications Data Link Monitor Feature Server Measurement Collection Started event functions as an informational alert that the POTS/Centrex (CTX)/telecommunications data link monitor (TDM) feature server measurement collection has started. The event is informational and no further action is required.

## **Plain Old Telephone Service/Centrex/Telecommunications Data Link Monitor Feature Server Measurement Collection Finished - Statistics (5)**

The Plain Old Telephone Service/Centrex/Telecommunications Data Link Monitor Feature Server Measurement Collection Finished event functions as an informational alert that the POTS/CTX/TDM feature server measurement collection has finished. The event is informational and no further action is required.

## **Advanced Intelligent Network Feature Server Measurement Collection Started - Statistics (6)**

The Advanced Intelligent Network Feature Server Measurement Collection Started event functions as an informational alert that the AIN feature server measurement collection has started. The event is informational and no further action is required.

## **Advanced Intelligent Network Feature Server Measurement Collection Finished - Statistics (7)**

The Advanced Intelligent Network Feature Server Measurement Collection Finished event functions as an informational alert that the AIN feature server measurement collection has finished. The event is informational and no further action is required.



## Message Send Failure - Statistics (8)

The Message Send Failure event serves as a warning that a message send has failed. The primary cause of the event is that the originating process (for CA, FS or EMS) is not in active state, or is shut down. To correct the primary cause of the event, check for other alarms and events generated from this component (CA, FS or EMS). The secondary cause of the event is that the hub is down. To correct the secondary cause of the event, is if the hub process is down, try to bring it into a normal state. The ternary cause of the event is that the platform is currently shutting down a process. To correct the ternary cause of the event, is if the originating process is down, try to bring the process back into the normal state. If this event report is being issued on every collection interval and there are no other event reports being issued, contact the Cisco TAC to resolve the communication issue. Refer to the [“Obtaining Technical Assistance” section on page xxxviii](#) for detailed instructions on contacting Cisco TAC and opening a service request.

Issued when the traffic measurement subsystem in the CA fails to send messages to the EMS due to:

- Originating process (for CA, FS or EMS) is not in active state, or is shut down.
- Hub is down.
- Platform is currently shutting down a process.

If this event is being issued frequently (every collection interval), then there are communication difficulties between the Call Agent and the EMS, and there will be additional events being issued. These other events will indicate the nature of the communication difficulties. The repair procedures for the other event reports should be followed to correct the Call Agent/EMS communication issue:

- Check for other alarms and events generated from this component (CA, FS or EMS).
- If the originating process is down, try to bring the process back into the normal state.
- If the hub process is down, try to bring it into a normal state.

If this event report is being issued on every collection interval and there are no other event reports being issued, contact the Cisco TAC to resolve the communication issue.

## Measurement Table Structured Query Language Read Error - Statistics (9)

The Measurement Table Structured Query Language Read Error event serves as a warning that the measurement table had a Structured Query Language (SQL) read error. The primary cause of the event is that there is no database connection, or the connection is faulty. To correct the primary cause of the event, check to see if there are any other events generated that indicate there is a database problem. The secondary cause of the event is that the traffic measurement tables are corrupted. To correct the secondary cause of the event, correct any database-related problems. The ternary cause of the event is that two processors or more are attempting to access the table at the same time. To correct the ternary cause of the event, check to see if all of the database-related problems are cleared, and this warning event report still occurs, contact Cisco TAC for technical support. Refer to the [“Obtaining Technical Assistance” section on page xxxviii](#) for detailed instructions on contacting Cisco TAC and opening a service request.

## Measurement Table Structured Query Language Write Error - Statistics (10)

The Measurement Table Structured Query Language Write Error event serves as a warning that the measurement table has had a SQL write error. The primary cause of the event is that there is no database connection, or the connection is faulty. To correct the primary cause of the event, check to see if there are any other events generated that indicate there is a database problem. The secondary cause of the event is that the traffic measurement tables are corrupted. To correct the secondary cause of the event, correct any database-related problems. The ternary cause of the event is that two processors or more are attempting to access the table at the same time. To correct the ternary cause of the event, check to see if all of the database-related problems are cleared, and this warning event report still occurs, contact Cisco TAC for technical support. Refer to the [“Obtaining Technical Assistance” section on page xxxviii](#) for detailed instructions on contacting Cisco TAC and opening a service request.

## Measurement Collection Application Programming Interface Failure - Statistics (11)

The Measurement Collection Application Programming Interface Failure event serves as a warning that the measurement collection of application programming interface (API) statistics has failed. The primary cause of the event is that the report is issued when the traffic measurement subsystem on the call agent or feature server encounters difficulties when it tries to collect measurement values from one of the processes. To correct the primary cause of the event execute a status command for the affected call agent or feature server. The secondary cause of the event is that the originating process (for CA, FS or EMS) is not in active state, or is shut down. To correct the secondary cause of the event, check and see if the status report indicates that the originating process is down, try to bring the process back into the normal (In Service) state. If you need assistance in restoring a process, contact Cisco TAC. The ternary cause of the event is that the platform is currently shutting down the originating process. To correct the ternary cause of the event, check and see if this event report is being issued every collection period, contact Cisco TAC for assistance. Refer to the [“Obtaining Technical Assistance” section on page xxxviii](#) for detailed instructions on contacting Cisco TAC and opening a service request.

**Note**

---

Traffic measurements will not be available for the affected call agent or feature server from the measurement period in which this event report was issued.

---

## Measurement Handshake Error - Schema Inconsistency - Statistics (12)

The Measurement Handshake Error - Schema Inconsistency alarm (major) indicates that a measurement handshake error has occurred. To troubleshoot and correct the cause of the Measurement Handshake Error - Schema Inconsistency alarm, refer to the [“Measurement Handshake Error - Schema Inconsistency - Statistics \(12\)” section on page 11-16](#).

## Traffic and Measurements Module Application Programming Interface Failure - Statistics (13)

The Traffic and Measurements Module Application Programming Interface Failure alarm (major) indicates that the Traffic and Measurements module (TMM) API failed. To troubleshoot and correct the cause of the Traffic and Measurements Module Application Programming Interface Failure alarm, refer to the [“Traffic and Measurements Module Application Programming Interface Failure - Statistics \(13\)” section on page 11-16](#).

# Troubleshooting Statistics Alarms

This section provides the information needed to monitor and correct Statistics alarms. [Table 11-3](#) lists all Statistics alarms in numerical order and provides cross reference to each subsection in this section.

**Table 11-3** *Cisco BTS 10200 Softswitch Statistics Alarms*

| Alarm Type     | Alarm Name                                                                                                  | Alarm Severity |
|----------------|-------------------------------------------------------------------------------------------------------------|----------------|
| STATISTICS(12) | <a href="#">Measurement Handshake Error - Schema Inconsistency - Statistics (12)</a>                        | MAJOR          |
| STATISTICS(13) | <a href="#">Traffic and Measurements Module Application Programming Interface Failure - Statistics (13)</a> | MAJOR          |

## Measurement Handshake Error - Schema Inconsistency - Statistics (12)

The Measurement Handshake Error - Schema Inconsistency alarm (major) indicates that a measurement handshake error has occurred. The primary cause of the alarm is that counters have been added or deleted from the schema in Oracle but not in the Call Agent. To correct the primary cause of the alarm, add or delete the counters on the CA. The secondary cause of the alarm is that the software load has been installed incorrectly. To correct the secondary cause of the alarm, re-install the software load.

## Traffic and Measurements Module Application Programming Interface Failure - Statistics (13)

The Traffic and Measurements Module Application Programming Interface Failure alarm (major) indicates that the TMM API failed. The primary cause of the alarm is that the system is unable to initialize the shared memory. To correct the primary cause of the alarm, reconfigure and restart the system. The secondary cause of the alarm is that a process is unable to attach to the shared memory. To correct the secondary cause of the alarm, restart the offending process. The tertiary cause of the alarm is that the shared memory table has overflowed. To correct the tertiary cause of the alarm, reconfigure/restart or fix problematic application. The subsequent cause of the alarm is that the shared memory is exhausted. To correct the subsequent cause of the alarm, reconfigure and restart the system.



## CHAPTER 12

# System Troubleshooting

---

Revised: October 23, 2008, OL-11335-06

## Introduction

This chapter provides the information needed to monitor and troubleshoot System events and alarms. This chapter is divided into the following sections:

- [System Events and Alarms](#) – Provides a brief overview of each System event and alarm.
- [Monitoring System Events](#) – Provides the information needed to monitor and correct System events.
- [Troubleshooting System Alarms](#) – Provides the information needed to troubleshoot and correct System alarms.

# System Events and Alarms

This section provides a brief overview of the System events and alarms for the Cisco BTS 10200 Softswitch in numerical order. [Table 12-1](#) lists all of the System events and alarms by severity.



Note

Click the System message number in [Table 12-1](#) to display information about the event or alarm.

Table 12-1 System Events and Alarms by Severity

| CRITICAL | MAJOR                       | MINOR                       | WARNING                    | INFO                       |
|----------|-----------------------------|-----------------------------|----------------------------|----------------------------|
|          | <a href="#">SYSTEM (8)</a>  | <a href="#">SYSTEM (2)</a>  | <a href="#">SYSTEM (5)</a> | <a href="#">SYSTEM (1)</a> |
|          | <a href="#">SYSTEM (12)</a> | <a href="#">SYSTEM (3)</a>  | <a href="#">SYSTEM (9)</a> |                            |
|          |                             | <a href="#">SYSTEM (4)</a>  |                            |                            |
|          |                             | <a href="#">SYSTEM (6)</a>  |                            |                            |
|          |                             | <a href="#">SYSTEM (7)</a>  |                            |                            |
|          |                             | <a href="#">SYSTEM (10)</a> |                            |                            |
|          |                             | <a href="#">SYSTEM (11)</a> |                            |                            |

## SYSTEM (1)

For additional information, refer to the “[Test Report - System \(1\)](#)” section on page 12-9.

|                |                                                      |
|----------------|------------------------------------------------------|
| DESCRIPTION    | Test Report                                          |
| SEVERITY       | Information (INFO)                                   |
| THRESHOLD      | 100                                                  |
| THROTTLE       | 0                                                    |
| PRIMARY CAUSE  | This is a test report for the new “SYSTEM” category. |
| PRIMARY ACTION | No action is required.                               |

## SYSTEM (2)

To troubleshoot and correct the cause of the alarm, refer to the [“Inter-Process Communication Queue Read Failure - System \(2\)”](#) section on page 12-12.

|                |                                                                                         |
|----------------|-----------------------------------------------------------------------------------------|
| DESCRIPTION    | Inter-Process Communication Queue Read Failure (IPC Queue Read Failure)                 |
| SEVERITY       | MINOR                                                                                   |
| THRESHOLD      | 100                                                                                     |
| THROTTLE       | 0                                                                                       |
| DATAWORDS      | Queue Name - STRING [20]<br>Location Tag - STRING [30]                                  |
| PRIMARY CAUSE  | There is a problem with inter-process communication (IPC) communication.                |
| PRIMARY ACTION | If problem persists, call Cisco Technical Assistance Center (TAC). (Contact Cisco TAC.) |

Refer to the [“Obtaining Technical Assistance”](#) section on page xxxviii for detailed instructions on contacting Cisco TAC and opening a service request.

## SYSTEM (3)

To troubleshoot and correct the cause of the alarm, refer to the [“Inter-Process Communication Message Allocate Failure - System \(3\)”](#) section on page 12-12.

|                |                                                                                               |
|----------------|-----------------------------------------------------------------------------------------------|
| DESCRIPTION    | Inter-Process Communication Message Allocate Failure (IPC Message Allocate Failure)           |
| SEVERITY       | MINOR                                                                                         |
| THRESHOLD      | 100                                                                                           |
| THROTTLE       | 0                                                                                             |
| DATAWORDS      | Requested Size - TWO_BYTES<br>Error Code - FOUR_BYTES<br>Location Tag - STRING [30]           |
| PRIMARY CAUSE  | There is a system error or there is not enough free memory left to allocate a message buffer. |
| PRIMARY ACTION | If problem persists, call Cisco TAC. (Contact Cisco TAC.)                                     |

Refer to the [“Obtaining Technical Assistance”](#) section on page xxxviii for detailed instructions on contacting Cisco TAC and opening a service request.

## SYSTEM (4)

To troubleshoot and correct the cause of the alarm, refer to the [“Inter-Process Communication Message Send Failure - System \(4\)”](#) section on page 12-12.

|                  |                                                                                                                          |
|------------------|--------------------------------------------------------------------------------------------------------------------------|
| DESCRIPTION      | Inter-Process Communication Message Send Failure (IPC Message Send Failure)                                              |
| SEVERITY         | MINOR                                                                                                                    |
| THRESHOLD        | 50                                                                                                                       |
| THROTTLE         | 0                                                                                                                        |
| DATAWORDS        | Error Code - FOUR_BYTES<br>Destination Process - FOUR_BYTES<br>Message Number - FOUR_BYTES<br>Location Tag - STRING [30] |
| PRIMARY CAUSE    | The process for which the message is intended is not running.                                                            |
| PRIMARY ACTION   | Check to ensure all components/processes are running. Attempt to restart any component/process that is not.              |
| SECONDARY CAUSE  | An internal error has occurred.                                                                                          |
| SECONDARY ACTION | If problem persists, call Cisco TAC. (Contact Cisco TAC.)                                                                |

Refer to the [“Obtaining Technical Assistance”](#) section on page xxxviii for detailed instructions on contacting Cisco TAC and opening a service request.



## SYSTEM (5)

To monitor and correct the cause of the event, refer to the [“Unexpected Inter-Process Communication Message Received - System \(5\)” section on page 12-10.](#)

|                |                                                                                                                             |
|----------------|-----------------------------------------------------------------------------------------------------------------------------|
| DESCRIPTION    | Unexpected Inter-Process Communication Message Received (Unexpected IPC Message Received)                                   |
| SEVERITY       | WARNING                                                                                                                     |
| THRESHOLD      | 100                                                                                                                         |
| THROTTLE       | 0                                                                                                                           |
| DATAWORDS      | Source Process Type - ONE_BYTE<br>Source Thread Type - ONE_BYTE<br>Message Number - TWO_BYTES<br>Location Tag - STRING [30] |
| PRIMARY CAUSE  | The process reporting the event is receiving messages it is not expecting.                                                  |
| PRIMARY ACTION | Call Cisco TAC. (Contact Cisco TAC.)                                                                                        |

Refer to the [“Obtaining Technical Assistance” section on page xxxviii](#) for detailed instructions on contacting Cisco TAC and opening a service request.

## SYSTEM (6)

To troubleshoot and correct the cause of the alarm, refer to the [“Index List Insert Error - System \(6\)” section on page 12-13.](#)

|                |                                                                                            |
|----------------|--------------------------------------------------------------------------------------------|
| DESCRIPTION    | Index List Insert Error (IDX List Insert Error)                                            |
| SEVERITY       | MINOR                                                                                      |
| THRESHOLD      | 100                                                                                        |
| THROTTLE       | 0                                                                                          |
| DATAWORDS      | List Name - STRING [20]<br>Index of Entry Being - FOUR_BYTES<br>Location Tag - STRING [30] |
| PRIMARY CAUSE  | An internal error has occurred.                                                            |
| PRIMARY ACTION | If problem persists, call Cisco TAC. (Contact Cisco TAC.)                                  |

Refer to the [“Obtaining Technical Assistance” section on page xxxviii](#) for detailed instructions on contacting Cisco TAC and opening a service request.

## SYSTEM (7)

To troubleshoot and correct the cause of the alarm, refer to the [“Index List Remove Error - System \(7\)” section on page 12-13](#).

|                |                                                                                            |
|----------------|--------------------------------------------------------------------------------------------|
| DESCRIPTION    | Index List Remove Error (IDX List Remove Error)                                            |
| SEVERITY       | MINOR                                                                                      |
| THRESHOLD      | 100                                                                                        |
| THROTTLE       | 0                                                                                          |
| DATAWORDS      | List Name - STRING [20]<br>Index of Entry Being - FOUR_BYTES<br>Location Tag - STRING [30] |
| PRIMARY CAUSE  | An internal error has occurred.                                                            |
| PRIMARY ACTION | If problem persists, call Cisco TAC. (Contact Cisco TAC.)                                  |

Refer to the [“Obtaining Technical Assistance” section on page xxxviii](#) for detailed instructions on contacting Cisco TAC and opening a service request.

## SYSTEM (8)

To troubleshoot and correct the cause of the alarm, refer to the [“Thread Creation Failure - System \(8\)” section on page 12-13](#).

|                |                                                                                                                         |
|----------------|-------------------------------------------------------------------------------------------------------------------------|
| DESCRIPTION    | Thread Creation Failure                                                                                                 |
| SEVERITY       | MAJOR                                                                                                                   |
| THRESHOLD      | 100                                                                                                                     |
| THROTTLE       | 0                                                                                                                       |
| DATAWORDS      | Error Code - FOUR_BYTES<br>Thread Name - STRING [20]<br>Location Tag - STRING [30]                                      |
| PRIMARY CAUSE  | An internal error has occurred. A process was unable to create one of its threads.                                      |
| PRIMARY ACTION | Attempt to restart the node on which the error occurred. If the same error occurs, call Cisco TAC. (Contact Cisco TAC.) |

Refer to the [“Obtaining Technical Assistance” section on page xxxviii](#) for detailed instructions on contacting Cisco TAC and opening a service request.

## SYSTEM (9)

To monitor and correct the cause of the event, refer to the [“Timer Start Failure - System \(9\)”](#) section on page 12-10.

|                |                                                           |
|----------------|-----------------------------------------------------------|
| DESCRIPTION    | Timer Start Failure                                       |
| SEVERITY       | WARNING                                                   |
| THRESHOLD      | 100                                                       |
| THROTTLE       | 0                                                         |
| DATAWORDS      | Timer Type - STRING [20]<br>Location Tag - STRING [30]    |
| PRIMARY CAUSE  | Process was unable to start a platform timer.             |
| PRIMARY ACTION | If problem persists, call Cisco TAC. (Contact Cisco TAC.) |

Refer to the [“Obtaining Technical Assistance”](#) section on page xxxviii for detailed instructions on contacting Cisco TAC and opening a service request.

## SYSTEM (10)

To troubleshoot and correct the cause of the alarm, refer to the [“Index Update Registration Error - System \(10\)”](#) section on page 12-13.

|                |                                                                                   |
|----------------|-----------------------------------------------------------------------------------|
| DESCRIPTION    | Index Update Registration Error (IDX Update Registration Error)                   |
| SEVERITY       | MINOR                                                                             |
| THRESHOLD      | 100                                                                               |
| THROTTLE       | 0                                                                                 |
| DATAWORDS      | Error Code - FOUR_BYTES<br>Table Name - STRING [20]<br>Location Tag - STRING [30] |
| PRIMARY CAUSE  | Application unsuccessfully requested to be notified of table changes.             |
| PRIMARY ACTION | Call Cisco TAC. (Contact Cisco TAC.)                                              |

Refer to the [“Obtaining Technical Assistance”](#) section on page xxxviii for detailed instructions on contacting Cisco TAC and opening a service request.

## SYSTEM (11)

To troubleshoot and correct the cause of the alarm, refer to the [“Index Table Add Entry Error - System \(11\)” section on page 12-13](#).

|                |                                                                                                                        |
|----------------|------------------------------------------------------------------------------------------------------------------------|
| DESCRIPTION    | Index Table Add Entry Error (IDX Table Add-Entry Error)                                                                |
| SEVERITY       | MINOR                                                                                                                  |
| THRESHOLD      | 100                                                                                                                    |
| THROTTLE       | 0                                                                                                                      |
| DATAWORDS      | Table Name - STRING [20]<br>Index of Entry Being - FOUR_BYTES<br>Error Code - FOUR_BYTES<br>Location Tag - STRING [30] |
| PRIMARY CAUSE  | An internal error has occurred.                                                                                        |
| PRIMARY ACTION | If problem persists, call Cisco TAC. (Contact Cisco TAC.)                                                              |

Refer to the [“Obtaining Technical Assistance” section on page xxxviii](#) for detailed instructions on contacting Cisco TAC and opening a service request.

## SYSTEM (12)

To troubleshoot and correct the cause of the alarm, refer to the [“Software Error - System \(12\)” section on page 12-13](#).

|                |                                                                                                                                            |
|----------------|--------------------------------------------------------------------------------------------------------------------------------------------|
| DESCRIPTION    | Software Error                                                                                                                             |
| SEVERITY       | MAJOR                                                                                                                                      |
| THRESHOLD      | 100                                                                                                                                        |
| THROTTLE       | 0                                                                                                                                          |
| DATAWORDS      | Context Description - STRING [80]<br>FileName - STRING [20]<br>Line Number of Code - TWO_BYTES<br>Error Specific Information - STRING [80] |
| PRIMARY CAUSE  | Logic path is not handled by algorithm in code.                                                                                            |
| PRIMARY ACTION | Save trace log around the time of occurrence and notify Cisco Systems, Inc. (Contact Cisco TAC.)                                           |

Refer to the [“Obtaining Technical Assistance” section on page xxxviii](#) for detailed instructions on contacting Cisco TAC and opening a service request.

# Monitoring System Events

This section provides the information needed to monitor and correct System events. [Table 12-2](#) lists all System events in numerical order and provides cross reference to each subsection in this section.

**Table 12-2** Cisco BTS 10200 Softswitch System Events

| Event Type | Event Name                                                                           | Event Severity |
|------------|--------------------------------------------------------------------------------------|----------------|
| SYSTEM(1)  | <a href="#">Test Report - System (1)</a>                                             | INFO           |
| SYSTEM(2)  | <a href="#">Inter-Process Communication Queue Read Failure - System (2)</a>          | MINOR          |
| SYSTEM(3)  | <a href="#">Inter-Process Communication Message Allocate Failure - System (3)</a>    | MINOR          |
| SYSTEM(4)  | <a href="#">Inter-Process Communication Message Send Failure - System (4)</a>        | MINOR          |
| SYSTEM(5)  | <a href="#">Unexpected Inter-Process Communication Message Received - System (5)</a> | WARNING        |
| SYSTEM(6)  | <a href="#">Index List Insert Error - System (6)</a>                                 | MINOR          |
| SYSTEM(7)  | <a href="#">Index List Remove Error - System (7)</a>                                 | MINOR          |
| SYSTEM(8)  | <a href="#">Thread Creation Failure - System (8)</a>                                 | MAJOR          |
| SYSTEM(9)  | <a href="#">Timer Start Failure - System (9)</a>                                     | WARNING        |
| SYSTEM(10) | <a href="#">Index Update Registration Error - System (10)</a>                        | MINOR          |
| SYSTEM(11) | <a href="#">Index Table Add-Entry Error - System (11)</a>                            | MINOR          |
| SYSTEM(12) | <a href="#">Software Error - System (12)</a>                                         | MAJOR          |

## Test Report - System (1)

The Test Report event is for testing the system event category. The event is informational and no further action is required.

## Inter-Process Communication Queue Read Failure - System (2)

The Inter-Process Communication Queue Read Failure alarm (minor) indicates that the IPC queue read has failed. To troubleshoot and correct the cause of the Inter-Process Communication Queue Read Failure alarm, refer to the [“Inter-Process Communication Queue Read Failure - System \(2\)”](#) section on [page 12-12](#).

## Inter-Process Communication Message Allocate Failure - System (3)

The Inter-Process Communication Message Allocate Failure alarm (minor) indicates that the IPC message allocation has failed. To troubleshoot and correct the cause of the Inter-Process Communication Message Allocate Failure alarm, refer to the [“Inter-Process Communication Message Allocate Failure - System \(3\)”](#) section on [page 12-12](#).

## Inter-Process Communication Message Send Failure - System (4)

The Inter-Process Communication Message Send Failure alarm (minor) indicates that the IPC message send has failed. To troubleshoot and correct the cause of the Inter-Process Communication Message Send Failure alarm, refer to the [“Inter-Process Communication Message Send Failure - System \(4\)” section on page 12-12](#).

## Unexpected Inter-Process Communication Message Received - System (5)

The Unexpected Inter-Process Communication Message Received event serves as a warning that an unexpected IPC message was received. The primary cause of the event is that the IPC process is receiving messages it is not expecting. To correct the primary cause of the event, contact Cisco TAC. Refer to the [“Obtaining Technical Assistance” section on page xxxviii](#) for detailed instructions on contacting Cisco TAC and opening a service request.

## Index List Insert Error - System (6)

The Index List Insert Error alarm (minor) indicates that an error has been inserted in the index list. To troubleshoot and correct the cause of the Index List Insert Error alarm, refer to the [“Index List Insert Error - System \(6\)” section on page 12-13](#).

## Index List Remove Error - System (7)

The Index List Remove Error alarm (minor) indicates that an index list remove error has occurred. To troubleshoot and correct the cause of the Index List Remove Error alarm, refer to the [“Index List Remove Error - System \(7\)” section on page 12-13](#).

## Thread Creation Failure - System (8)

The Thread Creation Failure alarm (major) indicates that a thread creation has failed. To troubleshoot and correct the cause of the Thread Creation Failure alarm, refer to the [“Thread Creation Failure - System \(8\)” section on page 12-13](#).

## Timer Start Failure - System (9)

The Timer Start Failure event serves as a warning that a timer start failure has occurred. The primary cause of the event is that the process was unable to start a platform timer. To correct the primary cause of the event, check and see if the problem persists. If the problem persists, call Cisco TAC. Refer to the [“Obtaining Technical Assistance” section on page xxxviii](#) for detailed instructions on contacting Cisco TAC and opening a service request.

## Index Update Registration Error - System (10)

The Index Update Registration Error alarm (minor) indicates that an index update registration error has occurred. To troubleshoot and correct the cause of the Index Update Registration Error alarm, refer to the [“Index Update Registration Error - System \(10\)” section on page 12-13](#).

## Index Table Add-Entry Error - System (11)

The Index Table Add-entry Error alarm (minor) indicates that an error occurred while adding an entry in the index table. To troubleshoot and correct the cause of the Index Table Add-entry Error alarm, refer to the [“Index Table Add Entry Error - System \(11\)” section on page 12-13](#).

## Software Error - System (12)

The Software Error alarm (major) indicates that a software error has occurred. To troubleshoot and correct the cause of the Software Error alarm, refer to the [“Software Error - System \(12\)” section on page 12-13](#).

# Troubleshooting System Alarms

This section provides the information needed to monitor and correct System alarms. [Table 12-3](#) lists all System alarms in numerical order and provides cross reference to each subsection in this section.

**Table 12-3** Cisco BTS 10200 Softswitch System Alarms

| Alarm Type | Alarm Name                                                                        | Alarm Severity |
|------------|-----------------------------------------------------------------------------------|----------------|
| SYSTEM(2)  | <a href="#">Inter-Process Communication Queue Read Failure - System (2)</a>       | MINOR          |
| SYSTEM(3)  | <a href="#">Inter-Process Communication Message Allocate Failure - System (3)</a> | MINOR          |
| SYSTEM(4)  | <a href="#">Inter-Process Communication Message Send Failure - System (4)</a>     | MINOR          |
| SYSTEM(6)  | <a href="#">Index List Insert Error - System (6)</a>                              | MINOR          |
| SYSTEM(7)  | <a href="#">Index List Remove Error - System (7)</a>                              | MINOR          |
| SYSTEM(8)  | <a href="#">Thread Creation Failure - System (8)</a>                              | MAJOR          |
| SYSTEM(10) | <a href="#">Index Update Registration Error - System (10)</a>                     | MINOR          |
| SYSTEM(11) | <a href="#">Index Table Add Entry Error - System (11)</a>                         | MINOR          |
| SYSTEM(12) | <a href="#">Software Error - System (12)</a>                                      | MAJOR          |

## Inter-Process Communication Queue Read Failure - System (2)

The Inter-Process Communication Queue Read Failure alarm (minor) indicates that the IPC queue read has failed. The primary cause of the alarm is that there is a problem with IPC communication. To correct the primary cause of the alarm, contact Cisco TAC. Refer to the [“Obtaining Technical Assistance” section on page xxxviii](#) for detailed instructions on contacting Cisco TAC and opening a service request.

## Inter-Process Communication Message Allocate Failure - System (3)

The Inter-Process Communication Message Allocate Failure alarm (minor) indicates that the IPC message allocation has failed. The primary cause of the alarm is that there is a system error, or there is not enough free memory left to allocate a message buffer. To correct the primary cause of the alarm, contact Cisco TAC. Refer to the [“Obtaining Technical Assistance” section on page xxxviii](#) for detailed instructions on contacting Cisco TAC and opening a service request.

## Inter-Process Communication Message Send Failure - System (4)

The Inter-Process Communication Message Send Failure alarm (minor) indicates that the IPC message send has failed. The primary cause of the alarm is that the process for which the message is intended is not running. To correct the primary cause of the alarm, check to ensure that all components and processes are running. Attempt to restart any component or process that is not running. The secondary cause of the alarm is that an internal error has occurred. To correct the secondary cause of the alarm, contact Cisco TAC. Refer to the [“Obtaining Technical Assistance” section on page xxxviii](#) for detailed instructions on contacting Cisco TAC and opening a service request.



## Index List Insert Error - System (6)

The Index List Insert Error alarm (minor) indicates that an error has been inserted in the index list. The primary cause of the alarm is that an internal error has occurred. To correct the primary cause of the alarm, contact Cisco TAC. Refer to the [“Obtaining Technical Assistance” section on page xxxviii](#) for detailed instructions on contacting Cisco TAC and opening a service request.

## Index List Remove Error - System (7)

The Index List Remove Error alarm (minor) indicates that an index list remove error has occurred. The primary cause of the alarm is that an internal error has occurred. To correct the primary cause of the alarm, contact Cisco TAC. Refer to the [“Obtaining Technical Assistance” section on page xxxviii](#) for detailed instructions on contacting Cisco TAC and opening a service request.

## Thread Creation Failure - System (8)

The Thread Creation Failure alarm (major) indicates that a thread creation has failed. The primary cause of the alarm is that an internal error occurred. A process was unable to create one of its threads. To correct the primary cause of the alarm, attempt to restart the node on which the error occurred. If the same alarm occurs, contact Cisco TAC. Refer to the [“Obtaining Technical Assistance” section on page xxxviii](#) for detailed instructions on contacting Cisco TAC and opening a service request.

## Index Update Registration Error - System (10)

The Index Update Registration Error alarm (minor) indicates that an index update registration error has occurred. The primary cause of the alarm is that an application unsuccessfully requested to be notified of table changes. To correct the primary cause of the alarm, contact Cisco TAC. Refer to the [“Obtaining Technical Assistance” section on page xxxviii](#) for detailed instructions on contacting Cisco TAC and opening a service request.

## Index Table Add Entry Error - System (11)

The Index Table Add Entry Error alarm (minor) indicates that an error occurred while adding an entry in the index table. The primary cause of the alarm is that an internal error has occurred. To correct the primary cause of the alarm, contact Cisco TAC. Refer to the [“Obtaining Technical Assistance” section on page xxxviii](#) for detailed instructions on contacting Cisco TAC and opening a service request.

## Software Error - System (12)

The Software Error alarm (major) indicates that a software error has occurred. The primary cause of the alarm is that a logic path is not handled by algorithm in the code. To correct the primary cause of the alarm, save the trace log from around the time of occurrence and contact Cisco TAC. Refer to the [“Obtaining Technical Assistance” section on page xxxviii](#) for detailed instructions on contacting Cisco TAC and opening a service request.





# CHAPTER 13

## Network Troubleshooting

---

Revised: October 23, 2008, OL-11335-06

### Introduction

The chapter provides the information needed to conduct network troubleshooting on the Cisco BTS 10200 Softswitch. For Signaling System 7 (SS7) network troubleshooting information refer to [Chapter 10, “Signaling Troubleshooting.”](#)



#### Caution

The use of the UNIX **ifconfig down** command on any signaling interface to test or troubleshoot network or interface failures of the Cisco BTS 10200 Softswitch Signaling Interface may lead to undesirable consequences or conditions.

---

### Troubleshooting a Network Failure

Network failure issues can be caused by several problems. This section describes the procedures to locate the cause of the problem. These procedures describe an iterative process that must be performed in order. When a problem is found and resolved, perform the procedure again from the beginning.

This section describes how to perform the following procedures:

- [Verify the Stream Control Transmission Protocol Association Status, page 13-2](#)
- [Verify the Configuration, page 13-3](#)
- [Verify the Internet Protocol Routing, page 13-5](#)
- [Verify if the Application Service Provider is Used by Any Application Server, page 13-5](#)
- [Verify the Internet Protocol Transfer Point T1 Card Provisioning, page 13-5](#)
- [Verify the Internet Protocol Transfer Point Message Transfer Part 2 Serial Interface, page 13-6](#)
- [Verify the Internet Protocol Transfer Point-Signal Transfer Point Linkset Status, page 13-7](#)
- [Verify the Internet Protocol Transfer Point Route, page 13-8](#)

# Verify the Stream Control Transmission Protocol Association Status

- Step 1** Determine if the administrative state and the operational state of the Stream Control Transmission Protocol (SCTP) association on the Cisco BTS 10200 Softswitch Element Management System (EMS) are in service. If the SCTP association is not in service, bring it in service and repeat this step. The following is an example of a healthy SCTP association:

```
CLI>status sctp-assoc id=sctp_assoc3

SCTP ASSOC ID -> sctp_assoc3
ADMIN STATE -> ADMIN_INS
OPER STATE -> SCTP-ASSOC in service
REASON -> ADM executed successfully
RESULT -> ADM configure result in success
```

Reply: Success:

- Step 2** Determine if the application service provider (ASP) is in service on the Cisco IP transfer point (ITP) by entering show cs7 asp name <asp-name>. The ASP name corresponds to the SCTP association name provisioned on the Cisco BTS 10200 Softswitch. Information similar to the following is displayed:

```
c2651-48#show cs7 asp name TB2-PRI-AIN
```

| ASP Name    | AS Name      | State    | Type | Rmt Port | Effect Remote IP | Primary Addr | SCTP |
|-------------|--------------|----------|------|----------|------------------|--------------|------|
| -----       | -----        | -----    | ---- | -----    | -----            | -----        | ---- |
| TB2-PRI-AIN | TB02-LNP-NC  | active   | SUA  | 12520    | 10.89.225.209    |              | 323  |
| TB2-PRI-AIN | TB02-SUALNP  | shutdown | SUA  | 12520    | 10.89.225.209    |              | 323  |
| TB2-PRI-AIN | TB02-800A-NC | active   | SUA  | 12520    | 10.89.225.209    |              | 323  |
| TB2-PRI-AIN | TB02-800T-NC | active   | SUA  | 12520    | 10.89.225.209    |              | 323  |
| TB2-PRI-AIN | TB02-SUA800A | active   | SUA  | 12520    | 10.89.225.209    |              | 323  |
| TB2-PRI-AIN | TB02-SUA800T | active   | SUA  | 12520    | 10.89.225.209    |              | 323  |

- If the status is shutdown, enter the following commands on the ITP and check the status again:

```
config terminal
cs7 asp <asp name>
no shut
```
- If the status of the ASP is inactive, the ASP is probably on the standby Cisco BTS 10200 Softswitch.
- If the ASP on the active Cisco BTS 10200 Softswitch is inactive, enter the following commands on the ITP and check the status again:

```
config terminal
cs7 asp <asp-name>
no shut
```
- If the ASP is now active, proceed to the [“Verify if the Application Service Provider is Used by Any Application Server”](#) section on page 13-5. Otherwise, continue to the next section.

## Verify the Configuration

- Step 1** Determine if the problem is an Internet Protocol (IP) address or port configuration mismatch between the ITP and the Cisco BTS 10200 Softswitch. Enter **show sctp-assoc id-<sctp-assoc-name>** on the Cisco BTS 10200 Softswitch EMS.
- Step 2** Enter **show cs7 sua** on the ITP.
- Step 3** Verify that the remote transport service access point (TSAP) address and the remote port of the SCTP association on the Cisco BTS 10200 Softswitch is the same as the local IP address and the local port used by the ITP SCCP user adapter (SUA). If the SCTP association is multi-homed, all of the IP addresses should be verified. The following example displays properly matched configurations:

```
CLI>show sctp-assoc id=sctp_assoc3
```

```
ID=sctp_assoc3
SGP_ID=itp_2651_1
SCTP_ASSOC_PROFILE_ID=sctp_prof
REMOTE_PORT=14001
REMOTE_TSAP_ADDR1=10.89.232.48
PLATFORM_ID=FSAIN520
DSCP=NONE
IP_TOS_PRECEDENCE=FLASH
LOCAL_RCVWIN=64000
MAX_INIT_RETRANS=5
MAX_INIT_RTO=1000
STATUS=INS
ULP=XUA
```

```
Reply: Success: Entry 1 of 1 returned.
```

```
c2651-48#show cs7 sua
Sigtran SUA draft version: 14
```

```
SUA Local port: 14001 State: active SCTP instance handle: 2
Local IP address: 10.89.232.48
Number of active SUA peers: 8
Max number of inbound streams allowed: 17
Local receive window: 64000
Max init retransmissions: 8
Max init timeout: 1000 ms
Unordered priority: equal
SCTP defaults for new associations
Transmit queue depth: 1000 Cumulative sack timeout: 200 ms
Assoc retransmissions: 10 Path retransmissions: 4
Minimum RTO: 1000 ms Maximum RTO: 1000 ms
Bundle status: on Bundle timeout: 400 ms
Keep alive status: true Keep alive timeout: 10000 ms
```

- Step 4** If there is no mismatch, proceed to Step 5. Otherwise, perform the following procedure:
- Correct the mismatch.
  - Bounce the SCTP association on the Cisco BTS 10200 Softswitch.
  - Repeat the [“Verify the Stream Control Transmission Protocol Association Status”](#) section on page 13-2.

**Step 5** Verify that the SCTP port on the Cisco BTS 10200 Softswitch and the remote port of the ASP on the ITP are the same.

- a. On the Cisco BTS 10200 Softswitch, open the platform.cfg file and locate the section for TCAP signaling adapter (TSA) on Feature Server for AIN services (FSAIN)/Feature Server for POTS, Tandem, and Centrex services (FSPTC), as illustrated in the following example:

```
[ProcessParameters]
ProcName=TSA
#----- Process priority (valid values = -60 to 60)
-----#
Priority=24
#----- Max thread priority (valid values = -60 to 60)
-----#
MaxDynamicThreadPriority=18
#-----Resource limits = (max descriptors) / (max heap size bytes) / (max stack size
bytes)-----#
ResourceLimits=0 / 524288000 / 0
ExecName=tsa.FSAIN520
ExecPath=./
Args=numthread 1 -tsadns crit-aSYS02AIN.ipclab.cisco.com -sctpport 12520 -stackcfg
tri_stack.cfg -multithread 0 -sgw_option SUA
ProcessGroup=0
ReportsDisableLevel=0
DebugReportsDisableLevel=0
NewConsole=0
Enable=1
ThreadHealthMonitoring=yes
SwitchOverIfMaxRestartExceededInDuplex=yes
EndPlatformIfMaxRestartExceededWhenMateFaulty=yes
#----- Restart rate = n / m (where n = Max restarts, m - interval in hours)
-----#
RestartRate=0 / 1
...
```

- b. On the ITP, enter **show run | begin <asp-name>**. Information similar to the following is displayed:

```
c2651-48#show run | begin TB2-PRI-AIN
cs7 asp TB2-PRI-AIN 12520 14001 sua
remote-IP 10.89.225.209
remote-IP 10.89.226.209
!
```

- c. If the sctpport on the Cisco BTS 10200 Softswitch and the remote port of the ASP on the ITP are the same, proceed to Step 6.
- d. If the sctpport on the Cisco BTS 10200 Softswitch and the remote port of the ASP on the ITP are not the same, perform the following procedure:
  - Correct the problem on the ITP
  - Bounce the SCTP association on the Cisco BTS 10200 Softswitch
  - Repeat the [“Verify the Stream Control Transmission Protocol Association Status”](#) section on page 13-2.

- Step 6** Verify that the tsadns resolves to exactly the same remote-IP as the ASP on the ITP. If not, perform the following procedures as necessary:
- Correct it in the /etc/hosts file and on the domain name system (DNS) server, if necessary.
  - Correct it on the ITP if the IP addresses on the ITP are incorrect.
  - Bounce the SCTP association on the Cisco BTS 10200 Softswitch.
  - Repeat the [“Verify the Stream Control Transmission Protocol Association Status”](#) section on page 13-2.

## Verify the Internet Protocol Routing

- Step 1** Ping the ITP addresses discovered in the [“Verify the Configuration”](#) section on page 13-3 from the Cisco BTS 10200 Softswitch in order to see if traffic is routed as planned.
- Step 2** Ping the Cisco BTS 10200 Softswitch addresses discovered in the [“Verify the Configuration”](#) section on page 13-3 from the ITP to see if traffic is routed as planned.
- Step 3** If routing is not as expected, correct the routing setup.
- Step 4** Repeat the [“Verify the Stream Control Transmission Protocol Association Status”](#) section on page 13-2.

## Verify if the Application Service Provider is Used by Any Application Server

If the ASP is not used by any application server (AS) in the ITP, the SCTP association will be taken down by the ITP. Make sure the AS using the ASP is provisioned before bringing up the SCTP association corresponding to the same ASP. If the ASP is used by any AS, continue to the next section. Otherwise, correct it and continue

## Verify the Internet Protocol Transfer Point T1 Card Provisioning

Enter **show controller t1 <slot/[bay/]port>** on the ITP. Verify if trunk level one (T1) is up. If not, check if the framing, line code, and the clock source are provisioned as planned. The following example displays a healthy card status:

```
c2651-48#show controllers t1 0/0

T1 0/0 is up.
 Applique type is Channelized T1
 Cablelength is short 133
 No alarms detected.
 alarm-trigger is not set
 Version info Firmware: 20010805, FPGA: 15
 Framing is ESF, Line Code is B8ZS, Clock Source is Line.
 Data in current interval (477 seconds elapsed):
 0 Line Code Violations, 0 Path Code Violations
 0 Slip Secs, 0 Fr Loss Secs, 0 Line Err Secs, 0 Degraded Mins
 0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs, 0 Unavail Secs
.....
```

## Verify the Internet Protocol Transfer Point Message Transfer Part 2 Serial Interface

To resolve problems with the ITP MTP2 serial interface, perform the following steps:

- Step 1** To display the state of the ITP MTP2 serial interface, enter **show int serial <number>** on the ITP. Information similar to the following will be displayed:

```
c2651-48#show int serial 0/0:0

Serial0/0:0 is up, line protocol is up
 Hardware is PowerQUICC Serial
 Description: link_to_mgts_lic_10
 MTU 1500 bytes, BW 56 Kbit, DLY 20000 usec,
 reliability 255/255, txload 1/255, rxload 1/255
 Encapsulation SS7 MTP2, loopback not set
 Keepalive not set
 Last input 33w5d, output 00:00:31, output hang never
 Last clearing of "show interface" counters 33w5d
 Queueing strategy: fifo
 Output queue 0/40, 0 drops; input queue 0/75, 23 drops
 30 second input rate 0 bits/sec, 0 packets/sec
 30 second output rate 0 bits/sec, 0 packets/sec
 1912000 packets input, 9866017 bytes, 0 no buffer
 Received 0 broadcasts, 0 runts, 17 giants, 0 throttles
 3356 input errors, 128 CRC, 2641 frame, 0 overrun, 0 ignored, 587 abort
 1163961 packets output, 13234709 bytes, 0 underruns
 0 output errors, 0 collisions, 55 interface resets
 0 output buffer failures, 0 output buffers swapped out
 31 carrier transitions
 Timeslot(s) Used:1, SCC: 0, Transmitter delay is 0 flags
```

- Step 2** If the interface is up and the line protocol is up, continue to the next section. If there is a problem, determine where the problem exists, as follows:
- If the interface is down, shut down the interface manually.
  - If the line protocol is down, the problem exists in cabling or in the MTP2 layer.
  - If both the interface and the line protocol are down, there is a hardware failure or the interface is manually shutdown.
- Step 3** After correcting the problem, continue to the next section.



## Verify the Internet Protocol Transfer Point-Signal Transfer Point Linkset Status

To resolve problems with the ITP-signal transfer point (STP) linkset status, perform the following steps:

- Step 1** Verify whether the link-set is available on the ITP by entering the following command

```
show cs7 linkset <ls-name>.
```

Information similar to the following is displayed:

```
c2651-48#show cs7 linkset
lsn=ls_to_mgts_lic_10 apc=1.101.0 state=avail avail/links=1/1
 SLC Interface Service PeerState Inhib
 00 Serial0/0:0 avail ----- -----
```

- Step 2** If the status is not available and at least one of the serial interfaces is available, the problem could be the point code type or point code value mismatch with the remote peer.

- Step 3** If the checking is successful, continue to the next section. Otherwise, correct the problem and continue.

## Verify the Internet Protocol Transfer Point Route

To resolve problems with the ITP route, perform the following steps:

- Step 1** Verify if there is a route to the destination point code provisioned in the Cisco BTS 10200 Softswitch by entering the following command:

```
show cs7 route
```

Information similar to the following is displayed:

```
c2651-48#show cs7 route
Dynamic Routes 0 of 500
```

```
Routing table = system Destinations = 6 Routes = 6
```

| Destination  |       | Prio | Linkset Name       | Route   |
|--------------|-------|------|--------------------|---------|
| 1.8.1/24     | INACC | 1    | ls_to_mgts_lic_10  | UNAVAIL |
| 1.12.1/24    | acces | 5    | ls_to_mgts_lic_10  | avail   |
| 1.101.0/24   | acces | 1    | ls_to_mgts_lic_10  | avail   |
| 7.44.120/24  | acces | 1    | ls_to_inet12_pod_1 | avail   |
| 7.44.121/24  | acces | 1    | ls_to_inet12_pod_1 | avail   |
| 7.212.112/24 | acces | 1    | ls_to_inet12_pod_1 | avail   |

```
Routing table = XUA
```

| Destination |       | Type |
|-------------|-------|------|
| 7.2.1/24    | acces | AS   |
| 7.2.3/24    | acces | AS   |
| 7.44.1/24   | acces | AS   |
| 7.44.3/24   | acces | AS   |

- Step 2** If the linkset is available and the route is UNAVAIL, the problem could be in the service provider's SS7 network. Contact the service provider to coordinate troubleshooting.

After successfully passing this step, the network failure should not happen. If it still happens, the supporting team or the developer should be contacted.



# CHAPTER 14

## General Troubleshooting

---

Revised: October 23, 2008, OL-11335-06

### Introduction

The chapter provides the general troubleshooting information needed to conduct troubleshooting on the Cisco BTS 10200 Softswitch. This chapter is divided into the following sections:

- [Troubleshooting CORBA Problems](#) – Provides a reference to the Common Object Request Broker Architecture (CORBA) troubleshooting information in the *Cisco BTS 10200 Softswitch CORBA Adapter Interface Specification Programmer Guide*.
- [Troubleshooting Local Number Portability Problems](#) – Provides the information to solve local number portability (LNP) problems.
- [Troubleshooting Alerting Notification Problems](#) – Explains how to troubleshoot the system when the 3PTYFS does not appear to be receiving the alerting notification and call data.
- [Command Responses](#) – Describes success and failure responses to commands, as well as values for the term-reason and trunk-reason responses.
- [Protocol Troubleshooting](#) – Provides the troubleshooting information for resolving Cisco BTS 10200 Softswitch protocol problems.



#### Caution

The use of the UNIX **ifconfig down** command on any signaling interface to test or troubleshoot network or interface failures of the Cisco BTS 10200 Softswitch Signaling Interface may lead to undesirable consequences or conditions.

---

### Troubleshooting CORBA Problems

To troubleshoot CORBA interface problems, refer to the *Cisco BTS 10200 Softswitch Release 4.1, 4.4.0, and 4.4.1 CORBA Adapter Interface Specification Programmer Guide, Chapter 5*.

# Troubleshooting Local Number Portability Problems

Problems can arise when porting a subscriber's telephone number from one service provider to another. The Network Interconnection Interoperability Forum (NIIF), a part of the Alliance for Telecommunications Industry Solutions (ATIS) organization, has published a document (ATIS/NIIF-0017) that includes detailed steps that service providers should follow when LNP problems are encountered. The document is titled *Guidelines for Reporting Local Number Portability Troubles in a Multiple Service Provider Environment*, and it is available at <http://www.atis.org/atis/clc/NIIF/niifdocs.htm>.

The NIIF also maintains the National LNP Contact Directory, a protected document that provides telephone numbers of 24 by 7 LNP-qualified contacts for each service provider. The directory is located at the URL given above. You can download and submit an application for a password at the same URL.

## Resolving Local Number Portability Conflicts

Some conflicts can arise in the LNP processes. [Figure 14-1](#) illustrates the causes of conflicts and the procedures that the Number Portability Administration Center (NPAC) service management system (SMS) uses to resolve them.

If either the old or new service provider did not send a notification to the NPAC SMS, the NPAC SMS notifies the service provider from which it did not receive a notification that it is expecting a notification. If the NPAC SMS receives the missing notification, and both notifications indicate agreement among the service providers, the process proceeds as normal.

The following list describes the actions that the NPAC SMS takes in different situations:

- If the NPAC SMS does *not* receive a concurring notification from the *old* service provider, the NPAC SMS logs the failure to respond and allows the new service provider to proceed with activation when the new service provider due date is reached.
- If the NPAC SMS does *not* receive a concurring notification from the *new* service provider, the NPAC SMS logs the failure to respond, cancels the request, and notifies both service providers of the cancellation.
- If the service providers disagree as to who will provide service for the telephone number, the NPAC SMS places the request in the “conflict” state and notifies both service providers of the conflict status and the Status Change Cause Code.
  - The service providers then determine between them who will serve the customer using their internal business processes.
  - When a resolution is reached, the NPAC SMS is notified by the new service provider and removes the request from the conflict state.

Within the first 6 hours, only the old service provider can initiate “conflict off.” After 6 hours, either service provider can remove the conflict status. The new service provider can alternatively request cancellation of the Subscription Version.

**Figure 14-1**      *Conflict Resolution Work Flow*

## Audit Requests

An audit function is necessary for troubleshooting customer problems and as a maintenance process to ensure Subscription Version data integrity across the entire LNP network. Audits are concerned with the process of comparing the NPAC SMS view of the LNP network's Subscription Version data with one or more of the service provider's views of its network.

The following methods help ensure data integrity across the LNP network:

- On-demand audits can be initiated by any service provider who believes a problem may exist in another service provider's network. These audits are executed through queries to the appropriate service provider's network, and corrected by means of downloads to those same networks.
- Local service providers are also responsible for comparing database extracts of Subscription data written to an File Transfer Protocol (FTP) site by the NPAC SMS with their own versions of the same Subscription data.
- The NPAC SMS selects a random sample of active Subscription Versions from its own database, then compares those samples to the representation of that same data in the various local SMS databases.

## Report Requests

The NPAC SMS supports report generation for predefined and ad hoc reports. The report generation function creates output report files according to specified format definitions, and distributes reports to output devices as requested. The report distribution service supports distribution to electronic files, to local or remote printers, to e-mail addresses, and to fax machines.

# Troubleshooting Alerting Notification Problems

This section explains how to troubleshoot the system when the 3PTYFS does not appear to be receiving the alerting notification and call data.

- Step 1** Verify that the ID, transport service access point (TSAP) ADDR, and TYPE are properly provisioned in the FEATURE-SERVER table.
- Step 2** Verify that the alerting notification feature (ALERT\_NOTIFY) is provisioned properly.
- Step 3** Verify one of the following two cases, as applicable:
  - Verify that the ALERT\_NOTIFY feature is included in the SERVICE table applicable to the specific subscriber.
  - Verify that the ALERT\_NOTIFY feature is included in the default office service ID (if the feature is intended to be offered to all subscribers on the switch).



**Note**

In the procedures included in this document, the alerting notification feature is provisioned using the feature identifier **FNAME=ALERT\_NOTIFY**. The feature identifier can be any unique string of up to 16 ASCII characters chosen by the service provider. If you are not sure of the name used in your system for this feature, use the **SHOW FEATURE** command and view the system response to find the name.

**Example:**

```
SHOW FEATURE-SERVER;
SHOW FEATURE FNAME=ALERT_NOTIFY;
SHOW CA-CONFIG TYPE=DEFAULT-OFFICE-SERVICE-ID;
SHOW SERVICE ID=<the value of the default-office-service-id>
SHOW SERVICE ID=6543;
SHOW SUBSCRIBER-SERVICE-PROFILE SERVICE-ID=6543;
```

- Step 4** If a TSAP address is used for the 3PTYFS, verify that the domain name is correctly provisioned in the DNS and resolves to the intended 3PTYFS.
- Step 5** Enter the CLI command to check for Signaling alarm #12—Feature Server is not up or is not responding to Call Agent. If this alarm is raised, there is a communications problem between the Cisco BTS 10200 Softswitch and the 3PTYFS.

**Example:**

```
show alarm type=signaling;
show alarm type=signaling; number=12;
```

The following details apply to SIGNALING alarm #12:

- For a 3PTYFS that is more than one hop away from the Cisco BTS 10200 Softswitch, SIGNALING alarm #12 is raised when communications between the Cisco BTS 10200 Softswitch and the first-hop node go down. However, the alarm is *not* raised if communications on the second (or more distant) hop go down, or if the DNS value for the 3PTYFS does not resolve correctly.
- The system can take up to two minutes to detect a communications failure in the first hop toward the 3PTYFS.

- Step 6** Verify that you have connectivity from the Cisco BTS 10200 Softswitch to the 3PTYFS.

- Step 7** Verify that the 3PTYFS is provisioned to support this feature in accordance with the applicable product documentation. The Cisco BTS 10200 Softswitch does not send any provisioning or status/control commands to the 3PTYFS.
- Step 8** Verify that the 3PTYFS and peripheral devices are operating properly according to the applicable product documentation.
- 

## Command Responses

This section describes success and failure responses to commands, as well as values for the term-reason and trunk-reason responses.

**Note**

In this section, an asterisk preceding a token name means the token is mandatory. A token without an asterisk is optional.

---

## Success and Failure Responses

The following message is returned upon the success of a command:

**Configuration Command Executed.**

One of the following responses can be returned upon the failure of a command:

- Administrative (ADM) found no failure.
- ADM MGW(s) cannot be found.
- ADM subscriber(s) cannot be found.
- ADM trunk group(s) cannot be found.
- ADM trunk(s) cannot be found.
- ADM no termination(s) found in MGW.
- ADM no trunk group(s) found in trunking gateway.
- ADM no trunk(s) found in trunk group.
- ADM fail while in termination table.
- ADM fail while in trunk group table.
- ADM fail while in trunk table.
- ADM fail while looking to find trunk index.
- ADM fail while getting MGW administration state.
- ADM fail while getting trunk group administration state.
- ADM fail while looking for MGW index.
- ADM administration state invalid.
- ADM failed to allocate inter-process communication (IPC) message(s).
- ADM failed to dispatch IPC message(s).
- ADM operational state invalid.
- ADM MGW(s) state change and pending.
- ADM subscriber(s) state change and pending.
- ADM trunk group(s) state change and pending.
- ADM trunk(s) state change and pending.
- ADM found subscriber category invalid.
- ADM found trunk group type invalid.
- ADM found trunk group state invalid.
- ADM found MGW admin state not ready.
- ADM found trunk group admin state not ready.
- ADM entity in desired state.
- ADM not allow trunk to reset.
- ADM not allow subscriber to reset.
- ADM change to out-of-service state required.
- ADM change to request graceful mode error.



- ADM found entity unequipped in initial state.
- ADM operation not allowed because D Channel(s) is down.
- The H.323 Gateway was not found in database management (DBM).
- ADM found unknown failure reason(s).

## Termination Reason Responses

The following responses can be returned for the termination reason (term-reason) response for subscriber termination and trunk termination commands:

- All of wildcard too complicated
- Channel-associated signaling (CAS) signaling protocol error
- Codec negotiation failure
- Endpoint does not have a digit map
- Endpoint malfunctioning
- Endpoint redirected to another Call Agent
- Endpoint taken out of service
- Error in RemoteConnectionDescriptor
- Event/signal parameter error
- Facility failure
- Failure of a grouping of trunks
- Incompatible protocol version
- Insufficient bandwidth at this time
- Insufficient bandwidth
- Internal consistency in local connection options
- Internal hardware failure.
- Invalid call ID
- Invalid conn identifier
- Invalid or unsupported command parameter
- Invalid or unsupported LocalConnectionOptions
- Loss of lower connectivity
- Loss of lower layer connectivity
- Manual intervention
- Missing remote connection descriptor
- Missing remote connection descriptor
- No fault reason available
- No such event or signal
- Packetization period not supported
- Per endpoint connection limit exceeded
- Quality of service (QoS) resource reservation was lost
- Response too big
- The media gateway is down
- The media gateway is in a faulty state
- The media gateway is transitioning to another state

- The media gateway is unreachable
- The phone is already off hook
- The phone is already on hook
- The transaction could not be executed because a protocol error was detected
- The transaction could not be executed because of internal overload
- The transaction could not be executed because the command contained an unrecognized extension
- The transaction could not be executed because the endpoint is not ready
- The transaction could not be executed because the endpoint is restarting
- The transaction could not be executed because the endpoint is unknown
- The transaction could not be executed because the gateway cannot send the specified announcement.
- The transaction could not be executed because the gateway is not equipped to detect one of the requested events
- The transaction could not be executed because the gateway is not equipped to generate one of the requested signals
- The transaction could not be executed, because the endpoint does not have sufficient resources at this time
- The transaction could not be executed, because the endpoint does not have enough resources available [permanent condition]
- The transaction could not be executed, because the endpoint is [restarting]
- The transaction could not be executed, due to a transient error
- The transaction could not be executed, due to some unspecified transient error
- The transaction could not be executed, endpoint does not have enough resources available
- The transaction has been queued. An actual completion message will follow later
- The transaction is currently being executed. An actual completion message will follow later
- The transaction refers to an incorrect connection-id
- The transaction refers to an unknown call Id
- The transaction time out
- The transaction was aborted by some external action
- Unknown action or illegal combination of actions
- Unknown extensions in local connection options
- Unknown or unsupported command
- Unknown or unsupported digit map extension
- Unknown or unsupported quarantine handling
- Unknown or unsupported RestartMethod
- Unsupported or invalid mode
- Unsupported or unknown package
- Unsupported values on local connection options

## Trunk Reason Responses

The following responses can be returned for the trunk reason (trunk-reason) response. One or more values can be returned, depending upon the operating conditions of the Call Agent.

- ACL\_CONGESTION\_LEVEL\_1—automatic congestion level (ACL) congestion is at level 1.
- ACL\_CONGESTION\_LEVEL\_2—ACL congestion is at level 2.
- ACL\_CONGESTION\_LEVEL\_3—ACL congestion is at level 3.
- DPC\_INACCESSIBLE—the DPC is not accessible.
- HARDWARE-BLOCK—trunk-termination is manually controlled OOS (controlled mode=FORCED).
- MAINT-BLOCK—trunk-termination is manually controlled OOS (controlled mode=GRACE).
- MAINT-BUSY—trunk-termination is in maintenance state; controlled to MAINT.
- MAINT-OOS—trunk-termination is manually controlled OOS. (There is no difference between this and a BLOCK.)
- NON-FAULTY—Not blocked, available for service.
- OUTGOING\_RESTRICTED—the outgoing call is not allowed.
- SIGNALLING-FAULT—Cannot exchange messages with public switched telephone network (PSTN) network:
  - dpc unavailable
  - user part unavailable
  - stcp association unavailable
  - Signaling link is faulty.
  - dpc congestion
- TERM-FAULT—Bearer termination is in faulty condition.
- TFC\_CONGESTION\_LEVEL\_1—Transfer controlled (TFC) congestion is at level 1.
- TFC\_CONGESTION\_LEVEL\_2—TFC congestion is at level 2.
- TFC\_CONGESTION\_LEVEL\_3—TFC congestion is at level 3.
- TFC\_INTL\_CONGESTION
- UNKNOWN\_REASON

## Trunk Termination Reason Responses, Signaling System 7 Only

The following responses can be returned for the trunk terminations on SS7 trunks. One or more values can be returned, depending upon the operating conditions of the Call Agent, in addition to the reason responses listed under [Trunk Reason Responses](#).

- **ACT\_LOC\_INIT\_RESET**—Reset circuit at startup as specified by command line argument for SGA process in the platform.cfg. Remains set until reset circuit (RSC)/group reset (GRS) and release complete (RLC)/group reset acknowledge (GRA) messages are exchanged with the remote switch.
- **ACT\_LOC\_MML\_RESET**—This is set when the reset command is issued from the CLI and remains set until reset is performed. Remains set until RSC/GRS and RLC/GRA messages are exchanged with the remote switch.
- **ACT\_LOC\_QUERY**—This is set when the a diagnostic command is issued from the CLI to perform a circuit query and remains set until circuit query message (CQM) and circuit query response (CQR) messages are exchanged with a remote switch.
- **ACT\_LOC\_UPU**—This is set when ITP informs that the user part is unavailable and remains set until a circuit verification response (CVR) is received or the ITP informs that the user part is available. The first incoming message will also clear this response.
- **ACT\_LOC\_VALIDATE**—This is set when the a diagnostic command is issued from the CLI to perform a circuit validation and remains set until circuit validation test (CVT) and CVR messages are exchanged with the remote switch.
- **ACT\_LOC\_COTTEST**—This is set when the a diagnostic command is issued from the CLI to perform a customer-originated trace (COT) test and remains set until SRINI TO CHECK messages are exchanged with the remote switch.
- **ACT\_LOC\_STOP**—This is set to clear a call when a term-fault is received.
- **BLK\_LOC\_UPU**—This is set when a trunk is blocked because user part is unavailable.
- **DES\_LOC\_GRACE**—Local hardware restart in progress (RSIP) graceful.
- **DES\_LOC\_SIG—SS7**—This is set when cannot exchange messages with PSTN network (a signaling fault):
  - dpc unavailable
  - user part unavailable
  - stcp association unavailable
  - Signaling link is faulty.
  - dpc congestion
- **SIGNALLING-FAULT**—This is set to indicate that the Cisco BTS 10200 Softswitch processed a DES\_LOC\_SIG—SS7 signaling fault.
- **DES\_LOC\_FORCE**—Local hardware failure.
- **DES\_LOC\_MML—MMLQ**—This is set when a control command is issued with mode=graceful and target-state=OOS. Also set during CQR processing.
- **DES\_LOC\_UPU**—This is set when user part is unavailable.
- **JOB\_PENDING**—Ongoing job in progress. There is an ongoing action of message exchange with the remote switch.
- **JOB\_REC**—Job was received by the message definition language (MDL) component and is being processed.

- OPER\_ACTIVE—Trunk is available for calls.
- REMOTE\_GRACE—Trunk is blocked remotely because of a CLI command on the remote switch.
- REMOTE\_FORCE—Trunk is blocked remotely because of a hardware failure on the remote switch.
- RESERVE\_SPARE1—Reserved for future use.
- RESERVE\_SPARE2—Reserved for future use.
- TERM\_GRACE—Trunk is gracefully blocked because of an RSIP graceful from the MGW.

## Fault Reason Responses

The following responses can be returned for the fault reason (fault-reason) response for a subscriber termination command. One or more values can be returned, depending upon the operating conditions of the Call Agent.

- The media gateway is down.
- The media gateway is unreachable.
- The media gateway is in a faulty state.
- The media gateway is transitioning to another state.
- The transaction could not be executed, due to a transient error.
- The transaction could not be executed because the endpoint is unknown.
- The transaction could not be executed because the endpoint is not ready.
- The transaction could not be executed, endpoint does not have enough resources available.
- The transaction could not be executed because a protocol error was detected.
- The transaction could not be executed because the command contained an unrecognized extension.
- The transaction could not be executed because the gateway is not equipped to detect one of the requested events.
- The transaction could not be executed because the gateway is not equipped to generate one of the requested signals.
- The transaction could not be executed because the gateway cannot send the specified announcement.
- Invalid conn identifier.
- Invalid call ID.
- Unsupported mode or invalid mode.
- Unsupported or unknown package.
- Endpoint does not have a digit map.
- The transaction could not be executed because the endpoint is restarting.
- Endpoint redirected to another Call Agent.
- No such event or signal.
- Unknown action or illegal combination of actions.
- Internal consistency in local connection options.
- Unknown extensions in local connection options.
- Insufficient bandwidth.
- Missing remote connection descriptor.
- Incompatible protocol version.
- Internal hardware failure.
- CAS signaling protocol error.
- Failure of a group of trunks.
- Unsupported values on local connection options.
- Response too big.

- Endpoint malfunctioning.
- Loss of lower connectivity.
- Endpoint taken out of service.
- No fault reason available.

## Protocol Troubleshooting

This section provides the troubleshooting information for resolving Cisco BTS 10200 Softswitch protocol problems.

### Troubleshooting Signaling System 7 SIGTRAN Problems

This section describes tools and procedures for troubleshooting SIGTRAN problems on the Cisco BTS 10200 Softswitch and Cisco ITP. It also describes how to clear SIGTRAN related Cisco BTS 10200 Softswitch alarms. In the descriptions within, a series of steps may be required to determine the source of the problem and may include viewing other alarms, invoking command-line interface (CLI) status and control commands, viewing the Cisco BTS 10200 Softswitch logs, and invoking ITP control and status requests.

For details on Cisco ITP operations, refer to the *Cisco IP Transfer Point Manual* at the following url:

<http://www.cisco.com/univercd/cc/td/doc/product/wireless/moblwrls/itp/>

This section contains the following sections:

- [Cisco Internet Protocol Transfer Point Troubleshooting Procedures](#)
- [Viewing Cisco BTS 10200 Softswitch Logs](#)
- [Troubleshooting Transaction Capabilities Application Part with the Query Verification Tool](#)

### Cisco Internet Protocol Transfer Point Troubleshooting Procedures

The following procedures are useful for troubleshooting problems on the Cisco ITP. This section contains the following procedures:

- [Internet Protocol Transfer Point System Messages](#)
- [Logging On to the Internet Protocol Transfer Point](#)
- [Viewing the Internet Protocol Transfer Point Configuration](#)
- [Internet Protocol Transfer Point Status Commands](#)
- [Controlling Internet Protocol Transfer Point Resources](#)

#### Internet Protocol Transfer Point System Messages

The Cisco ITP displays system messages when you are logged in to the console port. Some of these messages are similar to alarms. Analyzing ITP system messages is outside the scope of this document. For details concerning ITP system messages, please see the ITP Operations Manual at:

<http://www.cisco.com/univercd/cc/td/doc/product/wireless/moblwrls/itp/23sw/index.htm>



## Logging On to the Internet Protocol Transfer Point

Some of the troubleshooting sections in this chapter require the user to log on to the ITP. Access the ITP through the associated console server or through direct access with a console cable. You need the username and password to access the ITP.

Troubleshooting the ITP will require you to be in ITP enable mode. The enable mode is password protected. To get into enable mode, after logging in to the ITP, type **enable**. You will be prompted for the enable password.

## Viewing the Internet Protocol Transfer Point Configuration

To view the ITP configuration, log in to the ITP and get into enable mode. Enter the command **show run**. The configuration will be displayed. Continue to hit the enter key until you have viewed the entire configuration, or type “q” to stop viewing the configuration.

## Internet Protocol Transfer Point Status Commands

The following ITP commands are helpful for displaying the status of ITP resources:

- **show cs7 as**—Retrieves the application server (AS) status
- **show cs7 asp**—Retrieves the application service provider (ASP) status
- **show cs7 linkset**—Retrieves the Signaling System 7 (SS7) linkset status
- **show cs7 route**—Retrieves the SS7 route status
- **show cs7 group state**—Retrieves the signaling gateway (SG) group status

## Controlling Internet Protocol Transfer Point Resources

Change the administrative state of an ITP resource as follows:

- 
- |               |                                                                                                                     |
|---------------|---------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | Log on to the ITP, and get into configure mode.                                                                     |
| <b>Step 2</b> | Type the first configuration line of the resource that you want to control.                                         |
| <b>Step 3</b> | Type <b>shut</b> to take the resource out of service, or type <b>no-shut</b> to place the resource back in service. |
- 

The following example takes a linkset out of service:

```
va-2651-33#conf t
Enter configuration commands, one per line va-2651-33(config-cs7-ls)#

va-2651-33(config)#cs7 linkset lset1 1.1.20

va-2651-33(config-cs7-ls)#shut
*May 19 12:32:13.827: %CS7MTP3-5-ACTDEACTLINKSET: Linkset lset1 deactivation is in
progress
*May 19 12:32:13.827: %CS7MTP3-5-LINKUPDOWN: Link 0 in linkset lset1 is down
```

To put the linkset back in service, type the following command:

```
va-2651-33(config-cs7-ls)#no shut
*May 19 12:33:47.704: %CS7MTP3-5-ACTDEACTLINKSET: Linkset lset1 activation is in progress
*May 19 12:33:47.704: %CS7MTP3-5-ACTDEACTLINK: Link 0 linkset lset1 activation is in
progress
```

## Using Cisco BTS 10200 Softswitch Command Line Interface Commands

In the following sections, examples of Cisco BTS 10200 Softswitch CLI commands are used to aid in resolving Cisco BTS 10200 Softswitch alarms. The following CLI commands are helpful to display and clear alarms:

To display all the currently active alarms, enter the following command at a CLI prompt:

```
show alarm
```

To display all alarms of a specific type, enter:

```
show alarm type=<alarm type>
```

To clear an alarm, enter the following command:

```
clear alarm id=<alarm id>
```

For a detailed description of the CLI commands that are used, please see the *Cisco BTS 10200 Softswitch Command Line Interface Reference Guide, Release 4.5*, at the following universal resource locator (URL):

[http://www.cisco.com/univercd/cc/td/doc/product/voice/bts10200/bts4\\_5/cli/index.htm](http://www.cisco.com/univercd/cc/td/doc/product/voice/bts10200/bts4_5/cli/index.htm)

## Viewing Cisco BTS 10200 Softswitch Logs

Viewing Cisco BTS 10200 Softswitch logs is helpful when debugging MTP3 user adaptation (M3UA) related objects of the Cisco BTS 10200 Softswitch. Specific string patterns are printed out by the M3UA Interface Module and are useful to determine what is occurring in the log. These strings are formatted as follows:

```
MIM <functional area> <network object>
```

Functional areas include:

- Configuration (CFG)
- STATUS
- Protocol decode unit (PDU)
- STATISTICS
- Control (CTRL)
- PLATFORM

Network objects include:

- Stream Control Transmission Protocol (SCTP)
- Signaling gateway process (SGP)
- SG
- Destination point code (DPC)
- Originating point code (OPC)
- Routing key (RKEY)
- CC\_ROUTE

Search or grep the following example strings when searching the Cisco BTS 10200 Softswitch logs:

- M3UA Interface Module (MIM) CFG SCTP—Display how the SCTP has been configured at startup.
- MIM PDU—Trace incoming and outgoing ISUP messages at the MIM layer.
- MIM STATUS DPC—Display how the DPC status has changed in the system.
- MIM STATUS SCTP—Display how the SCTP status has changed in the system.
- MIM PLATFORM—Determine if a platform state change has been issued to the SGA/MIM module.
- MIM CTRL SCTP—Determine if an SCTP association has been administratively taken out of service or put back in service.

## Troubleshooting Transaction Capabilities Application Part with the Query Verification Tool

The Query Verification Tool (QVT) enables a user to generate Transaction Capabilities Application Part (TCAP) queries to external databases through the CLI interface. For information about the Query Verification Tool, refer to the following URL:

[http://www.cisco.com/univercd/cc/td/doc/product/voice/bts10200/bts4\\_4/featmods/qvttvt.htm#wp1168709](http://www.cisco.com/univercd/cc/td/doc/product/voice/bts10200/bts4_4/featmods/qvttvt.htm#wp1168709)

This section contains the following:

- [Table Configuration Problems](#)

## Table Configuration Problems

The CLI query command with the table-info option displays the tables used for routing the external SS7 queries on the Cisco BTS 10200 Softswitch. The query command can identify the following problems:

- Missing Call Agent (CA)-CONFIG table
- Missing SLHR-PROFILE table
- Missing Service Logic Host Route (SLHR) table
- Missing DPC table
- Missing OPC table
- Missing SUBSYSTEM-PROFILE table
- Missing SUBSYSTEM table
- Missing signaling connection control part (SCCP)-network (NW) table
- Missing SCCP-ROUTE table
- Missing ROUTING-KEY table
- Missing SG group (GRP) table
- Missing SG table
- Missing SGP table
- Missing SCTP-ASSOC table

To resolve a table error, add the appropriate entry to the table specified in the command response.

## Debugging Network Related Transaction Capabilities Application Part/Signaling Connection Control Part Problems

The CLI query command can provide information about network related problems. This section describes problems identified by the query command and the solutions to them.

This section contains the following:

- [No Translation for an Address of Such Nature](#)
- [No Translation for this Specific Address](#)
- [Subsystem Congestion](#)
- [Subsystem Failure](#)
- [Unequipped User](#)
- [Network Failure](#)
- [Network Congestion](#)
- [Unqualified](#)
- [Error In Message Transport](#)
- [Destination Cannot Perform Reassembly](#)
- [Signaling Connection Control Part Failure](#)
- [Segmentation Not Supported](#)
- [Segmentation Failure](#)
- [Query Verification Tool Timeout](#)
- [Command Line Interface Timeout](#)

### No Translation for an Address of Such Nature

|          |                                                                                |
|----------|--------------------------------------------------------------------------------|
| Layer    | SCCP                                                                           |
| Version  | ITU88, ITU92, ITU96, ANSI88, ANSI92                                            |
| Location | Signal transfer point (STP)                                                    |
| Cause    | The global text telephony (GTT) entry is not provisioned correctly in the STP. |
| Solution | Correct the GTT entry in the STP.                                              |

**No Translation for this Specific Address**

|          |                                                        |
|----------|--------------------------------------------------------|
| Layer    | SCCP                                                   |
| Version  | ITU88, ITU92, ITU96, ANSI88, ANSI92                    |
| Location | STP                                                    |
| Cause    | The GTT entry is not provisioned correctly in the STP. |
| Solution | Add the GTT entry in the STP.                          |

**Subsystem Congestion**

|          |                                                              |
|----------|--------------------------------------------------------------|
| Layer    | SCCP Subsystem (TCAP)                                        |
| Version  | ITU88, ITU92, ITU96, ANSI88, ANSI92                          |
| Location | Service control point (SCP)                                  |
| Cause    | The SCP subsystem is congested.                              |
| Solution | Ask the SCP Service Provider to solve the congestion problem |

**Subsystem Failure**

|          |                                                      |
|----------|------------------------------------------------------|
| Layer    | SCCP Subsystem (TCAP)                                |
| Version  | ITU88, ITU92, ITU96, ANSI88, ANSI92                  |
| Location | SCP                                                  |
| Cause    | The SCP is down or the subsystem of the SCP is down. |
| Solution | Verify that the SCP point code is correct.           |

## Unequipped User

|          |                                           |
|----------|-------------------------------------------|
| Layer    | SCCP Subsystem (TCAP)                     |
| Version  | ITU88, ITU92, ITU96, ANSI88, ANSI92       |
| Location | SCP                                       |
| Cause    | The SCCP user is not equipped             |
| Solution | Verify that the SCP point code is correct |

## Network Failure

|          |                                                                                                                   |
|----------|-------------------------------------------------------------------------------------------------------------------|
| Layer    | MTP3/MTP2/MTP1 or SCTP                                                                                            |
| Version  | ITU88, ITU92, ITU96, ANSI88, ANSI92 for MTP3/2/1, Internet Engineering Task Force (IETF) RFC 2960 for SCTP        |
| Location | Local, STP, or SCP                                                                                                |
| Cause    | The Broadband Telephony Softswitch (BTS)-ITP sctp-association is down or the SS7 link, linkset, or route is down. |
| Solution | See <a href="#">Chapter 13, “Network Troubleshooting,”</a> section assistance in solving this problem.            |

## Network Congestion

|          |                                                                                                                                                                                                                                                                                                              |
|----------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Layer    | SCCP                                                                                                                                                                                                                                                                                                         |
| Version  | ITU88, ITU92, ITU96, ANSI88, ANSI92                                                                                                                                                                                                                                                                          |
| Location | Local, STP, or SCP                                                                                                                                                                                                                                                                                           |
| Cause    | The SCTP layer or the SS7 network is congested.                                                                                                                                                                                                                                                              |
| Solution | The service provider of the SS7 network needs to either provide higher capacity or re-engineer the traffic. SCTP layer congestion normally indicates insufficient central processing unit (CPU) power. Hardware needs to be upgraded or more Cisco BTS 10200 Softswitch need to be added to offload traffic. |

**Unqualified**

|          |                                                       |
|----------|-------------------------------------------------------|
| Layer    | SCCP                                                  |
| Version  | ITU88, ITU92, ITU96, ANSI88, ANSI92                   |
| Location | STP or SCP                                            |
| Cause    | Unknown.                                              |
| Solution | Contact the support team or developer for assistance. |

**Error In Message Transport**

|          |                                                |
|----------|------------------------------------------------|
| Layer    | SCCP                                           |
| Version  | ITU92                                          |
| Location | STP                                            |
| Cause    | There was a failure in message transportation. |
| Solution | Contact the support team or the developer.     |

**Destination Cannot Perform Reassembly**

|          |                                                                                                                           |
|----------|---------------------------------------------------------------------------------------------------------------------------|
| Layer    | SCCP                                                                                                                      |
| Version  | ITU88, ITU92, ITU96, ANSI88, ANSI92                                                                                       |
| Location | SCP                                                                                                                       |
| Cause    | The peer side is not capable of reassembling extended unit data service (XUDTS) packets.                                  |
| Solution | The ITP does not support segmentation and reassembly. Contact the Cisco Technical Assistance Center (TAC) for assistance. |



### Signaling Connection Control Part Failure

|          |                                                                                                                                                                                                                                              |
|----------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Layer    | SCCP                                                                                                                                                                                                                                         |
| Version  | ITU88, ITU92, ITU96, ANSI88, ANSI92                                                                                                                                                                                                          |
| Location | Local, STP, or SCP                                                                                                                                                                                                                           |
| Cause    | The SCCP layer failed or the local TCAP signaling adapter (TSA) could not find the appropriate entry in the Subsystem table or the SCCP-nw table.                                                                                            |
| Solution | Add or properly populate the Subsystem and SCCP-nw tables. If it still does not work, restart the platform providing the service (Feature Server for AIN services (FSAIN) or Feature Server for POTS, Tandem, and Centrex services (FSPTC)). |

### Hop Counter Violation

|          |                                                                                                                                                      |
|----------|------------------------------------------------------------------------------------------------------------------------------------------------------|
| Layer    | SCCP                                                                                                                                                 |
| Version  | ITU96, ANSI92                                                                                                                                        |
| Location | STP                                                                                                                                                  |
| Cause    | The maximum hop count is exceeded during the message routing.                                                                                        |
| Solution | Make sure the hop count value provisioned in the SCCP-NW table is not too small. Verify that the SS7 network provider does not have any route-loops. |

### Segmentation Not Supported

|          |                                                                                             |
|----------|---------------------------------------------------------------------------------------------|
| Layer    | SCCP                                                                                        |
| Version  | ITU96                                                                                       |
| Location | SCP                                                                                         |
| Cause    | The peer side is not capable of reassembling XUDTS packets.                                 |
| Solution | The ITP does not support segmentation and reassembly. Contact the Cisco TAC for assistance. |

**Segmentation Failure**

|          |                                                                                             |
|----------|---------------------------------------------------------------------------------------------|
| Layer    | SCCP                                                                                        |
| Version  | ITU96                                                                                       |
| Location | STP                                                                                         |
| Cause    | The segmentation failed.                                                                    |
| Solution | The ITP does not support segmentation and reassembly. Contact the Cisco TAC for assistance. |

**Query Verification Tool Timeout**

|          |                                                                                                                                |
|----------|--------------------------------------------------------------------------------------------------------------------------------|
| Location | Local                                                                                                                          |
| Cause    | The SCP filed to respond or the TSA is out of service.                                                                         |
| Solution | If the SCP failed, contact the service provider to solve the problem. If the TSA is out of service, perform a manual failover. |

**Command Line Interface Timeout**

|          |                                                                                                                                                                                                                                                              |
|----------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Location | Local                                                                                                                                                                                                                                                        |
| Cause    | The Element Management System (EMS) and CA.FSAIN/FSPTC connection is down or the selective call acceptance (SCA) on the CA/FSAIN/FSPTC is out of service.                                                                                                    |
| Solution | If the SCA is down, restart the SCA or restart the platform where the SCA resides. If the EMS and CA/FSAIN/FSPTC connection is down, verify whether the Internet Protocol (IP) routing is correct and the OptiCall Messaging System (OMS) hub is in service. |

## Troubleshooting H.323 Problems

This section provides examples of possible problems you may encounter while working with H.323, and recommended solutions:

- [Outgoing Trunk Group is Out of Service](#)
- [Outgoing H.323 Gateway is Out of Service](#)
- [H.323 Gateway Fails to Register With Gatekeeper \(Invalid Alias\)](#)
- [Outgoing H.323 Gateway Unregistered With Gatekeeper and Needs to Use Registration, Admissions, and Status](#)
- [Stable Calls Are Dropped When Call Agent Switches Over](#)
- [No Matching Dial Plan Found on Incoming H.323 Trunk Group](#)
- [Configuration at Softswitch or Gatekeeper Has Placed Routing Into a Loop](#)
- [Outgoing H.323 Calls Routed to Incorrect Endpoint When Using Registration, Admissions, and Status](#)
- [Outgoing H.323 Calls Routed to Incorrect Endpoint When Using Direct Signaling](#)
- [Registration, Admissions, and Status Still Used When Outgoing H.323 Call is Provisioned to Use Direct Signaling](#)

### Outgoing Trunk Group is Out of Service

```
[I4 10:40:00.299 BCM 01-1 BCM_Main] "bcm_sel_term_tg_id(): get_tg_from_route() fail"
[bcm_bcsn_util.c:2614]
[***ERROR*** 10:40:00.299 BCM 01-1 BCM_Main] "Route Selection Failure"
[bcm_obcsn_sa_proc.c:3961]
```

This is an indication that the outgoing H.323 trunk group is out of service.

Verify the status of outgoing trunk group as follows:

```
CLI>status trunk_grp id=8991;
Reply : Success:

TGN ID -> 8991
ADMIN STATE -> ADMIN_OOS
OPER STATE -> Trunk group in-service
REASON -> ADM executed successful
RESULT -> ADM configure result in success
```

### Solution

Use CLI to place the trunk\_grp in-service as follows:

```
CLI> control trunk_grp id=8991; target-state=ins; mode=forced;
```

## Outgoing H.323 Gateway is Out of Service

```
[***WARNING*** 10:47:44.793 H3A3 01-1 Main] "Call failure H3A-->BCM sent for csaid=41
callid=0 reason=H323 gateway/gk seem to be OOS" [h3a_sig_sai.c:1525]
```

This is an indication that the outgoing H.323 gateway is “out of service”.

Verify the status of outgoing H.323 gateway:

```
CLI> status h323_gw id=CHINA_3;
Reply : Success:

ADMIN STATE -> ADMIN_OOS
H3A PROCESS NUMBER -> 32
H3A PROCESS NAME -> H3A3
ENDPOINT ID ->
ACTIVE CALLS -> 0
RAS STATE -> CCH323_RAS_STATE_NONE
RAS PORT -> 0
IP ADDRESS ->
REGISTERED GATEKEEPER ID -> NOT REGISTERED
PRIMARY GATEKEEPER ID ->
PRIMARY GATEKEEPER PORT -> 0
PRIMARY GATEKEEPER IP ->
H323 VERSION -> 4
TIME TO LIVE -> 0
NUM ALT GATEKEEPERS -> 0
ALT GATEKEEPER PERMANENT -> FALSE
THRESHOLD ENABLED -> FALSE
OUT OF RESOURCES -> FALSE
ALT GATEKEEPER LIST ->
```

### Solution

Use CLI to place the h323\_gw in-service as follows:

```
CLI> control h323_gw id=CHINA_3; target-state=ins;
Reply : Success: CLI change successful

H323GW ID -> CHINA_3
INITIAL STATE -> ADMIN_OOS
REQUEST STATE -> ADMIN_INS
RESULT STATE -> ADMIN_INS
FAIL REASON -> ADM found no failure
REASON -> ADM executed successful
RESULT -> ADM configure result in success
```

## H.323 Gateway Fails to Register With Gatekeeper (Invalid Alias)

When the H.323 gateway registers with a gatekeeper, sometimes an alias list is provided to the gatekeeper in the registration request (RRQ) message from gateway. Currently, this configuration is supported on Integrated Operating System (IOS) gateways (not in use on Cisco BTS 10200 Softswitch) when Foreign Exchange Station (FXS) ports are involved. If an request rejected (RRJ) message is received by gateway with reject reason of “invalidAlias”, this is symptomatic of an alias list being provided to the gatekeeper but the gatekeeper not configured to be responsible for the prefix associated with each of the aliases.

```
[+ . H3A3 . .] "value RasMessage ::= gatekeeperReject : "
[+ . H3A3 . .] " {"
[+ . H3A3 . .] " requestSeqNum 11"
[+ . H3A3 . .] " protocolIdentifier { 0 0 8 2250 0 3 }"
[+ . H3A3 . .] " rejectReason invalidAlias : NULL"
[+ . H3A3 . .] " }"
```

- Example:

Local gatekeeper that gateway is trying to register with configured as follows:

- zone prefix China-GK 30\*
- zone prefix China-GK 281\*
- zone prefix China-GK 29\*

Gateway has the following aliases that it wishes to register with:

c2620.50#show gateway

Gateway China-GW1 is not registered to any gatekeeper

Alias list (CLI configured)

- E164-ID 20751101
- E164-ID 20751102
- E164-ID 20751103
- E164-ID 20751104

In this case, China-GK does not have a prefix to match any of the E164 numbers.

### Solution

Add a zone prefix entry to China-GK that would cause a match on the alias numbers that are trying to be registered as follows:

- zone prefix China-GK 20\*

## Outgoing H.323 Gateway Unregistered With Gatekeeper and Needs to Use Registration, Admissions, and Status

```
[I4 10:52:44.824 H3A3 01-1 Lib_DBM] "H3A: h3a_use_ras Checking for RAS" [h3a_dbm.c:543]
[I4 10:52:44.824 H3A3 01-1 Lib_DBM] "h3a_get_dest_ip_addr: Need to use RAS"
[h3a_dbm.c:484]
[4? 10:52:44.824 H3A3 01-1 H_EVT] ": for callID 5 <cch323_call_setup_normal in
gw/src/cch323_gw_api.c:4247>"
[bts/os/src/bts_debug.c:200]
[4? 10:52:44.824 H3A3 01-1 H_225_EVT] "H.225 SM: process event H225_EVENT_RAS_RESOLVE,
for callID 5 <cch323_send
_event_to_h225 in gw/src/cch323_h225.c:337>" [bts/os/src/bts_debug.c:200]
[4? 10:52:44.824 H3A3 01-1 H_225_EVT] "cch323_run_h225_sm: received event
H225_EVENT_RAS_RESOLVE while at state
H225_IDLE <cch323_run_h225_sm in gw/src/cch323_h225.c:10085>" [bts/os/src/bts_debug.c:200]
[4? 10:52:44.824 H3A3 01-1 H_EVT] ": state = 0 <cch323_traverse_enum_contact_list in
gw/src/cch323_gw_api.c:
4652>" [bts/os/src/bts_debug.c:200]
[I3 10:52:44.824 H3A3 01-1 Main] "Rel message from STACK--->H3A for callid=5, cause
code=16" [h3a_sig_sai.c:1549]
```

This is an indication that the outgoing H.323 gateway needs to use Registration, Admissions, and Status (RAS) to complete the call, but because the gateway is not registered with a gatekeeper, the call is released.

Verify the status of the H.323 gateway with CLI command as follows:

```
CLI>status h323_gw id=CHINA_3;
Reply : Success:

ADMIN STATE -> ADMIN_INS
H3A PROCESS NUMBER -> 32
H3A PROCESS NAME -> H3A3
ENDPOINT ID ->
ACTIVE CALLS -> 0
RAS STATE -> CCH323_RAS_STATE_GRQ
RAS PORT -> 59723
IP ADDRESS -> 10.89.225.165
REGISTERED GATEKEEPER ID -> NOT REGISTERED
PRIMARY GATEKEEPER ID -> China-GK
PRIMARY GATEKEEPER PORT -> 1719
PRIMARY GATEKEEPER IP -> 10.89.227.198
H323 VERSION -> 4
TIME TO LIVE -> 0
NUM ALT GATEKEEPERS -> 0
ALT GATEKEEPER PERMANENT -> TRUE
THRESHOLD ENABLED -> FALSE
OUT OF RESOURCES -> FALSE
ALT GATEKEEPER LIST -> CLI>status h323_gw id=CHINA_3;
```

This shows that the H.323 gateway is in service, but it is not registered with a gatekeeper. The following are possible reasons for this: Incorrect provisioning for H323\_GW2GK (incorrect gatekeeper (GK) name, incorrect GK IP address, security violation) ---- this can be verified by trace logs as a gatekeeper reject (GRJ) would be sent back by GK as follows:

```
[+ . H3A3 . .] "value RasMessage ::= gatekeeperReject : "
[+ . H3A3 . .] " { "
[+ . H3A3 . .] " requestSeqNum 11"
[+ . H3A3 . .] " protocolIdentifier { 0 0 8 2250 0 3 }"
[+ . H3A3 . .] " rejectReason terminalExcluded : NULL"
[+ . H3A3 . .] " }"
```

Gatekeeper is down (no alternate GK or alternate is also down) --- this can be verified by trace logs as a timeout would occur (waiting for gatekeeper confirmation (GCF) or GRJ) after the H.323 gatekeeper request (GRQ) has been sent.

## Stable Calls Are Dropped When Call Agent Switches Over

If Annex E functionality is provisioned on the Cisco BTS 10200 Softswitch, but stable calls are being dropped when the H.323 process restarts or CA switches over, check to see whether configuration is correctly registered with the GK:

- 
- Step 1** Log on to gatekeeper
- Step 2** # show gatekeeper endpoints
- Step 3** Examine the display of the GK, which should look similar to the example below:

| CallSignalAddr  | Port | RASignalAddr    | Port  | Zone Name | Type              | Flags |
|-----------------|------|-----------------|-------|-----------|-------------------|-------|
| aaa.bbb.ccc.ddd | 1234 | eee.fff.ggg.hhh | 12345 | City GK   | VOIP-gateway (GW) | E     |
| iii.jjj.kkk.lll | 5678 | ppp.qqq.rrr.sss | 56789 | City GK   | VOIP-GW           | E     |

- Step 4** Verify that both the CA and H.323 Protocol (H323)-GW are registered with the GK with Flags=E as shown in the above example.
- 

## No Matching Dial Plan Found on Incoming H.323 Trunk Group

```
[I2 14:45:24.288 BCM 01-1 Lib_RTM] "dial_plan(pclId=45145211, dp_idx=0): no match"
[rtm_dial_plan.c:492]
[***ERROR*** 14:45:24.288 BCM 01-1 BCM_Main] "No Dial Plan Entry for digits in dial plan
0" [bcm_obcsm_sa_proc.c:8916]
```

After the SETUP message has been received at incoming H.323 gateway, Basic Call module (BCM) uses the dial\_plan\_id in the incoming trunk group and the called number to find out how to route the call. If no match is found, then this error will be issued.

### Solution

Add an entry to dial\_plan for called number and assign the identification (ID) to incoming trunk\_grp.

```
CLI> add dial_plan id=cdp1; digit_string=451452; dest_id=ipdest; min_digits=7;
max_digits=10;
CLI> change trunk_grp id=8991; dial_plan_id=cdp1;
```

## Configuration at Softswitch or Gatekeeper Has Placed Routing Into a Loop

```
[I5 10:16:20.921 BCM 01-1 BCM_Main] "BCM:TPM:Incr Counter(3):4199302144"
[bcm_tpm_proc.c:106]
[***ERROR*** 10:16:20.921 H3A3 01-1 Main] "alarm=99 reason=<Loop detected!!> call cleared
for callid=1
39 " [h3a_alarms.c:281]
```

### Solution

The routing problem could be in either the gatekeeper or the Cisco BTS 10200 Softswitch. Check the gatekeeper against the dialedDigits pattern in the admission request (ARQ), example:

```
destinationInfo "
[+ . H3A3 . .] " {"
[+ . H3A3 . .] " dialedDigits : "9991231234" "
[+ . H3A3 . .] " }"
```

There are multiple ways that a gatekeeper could determine the destCallSignalAddress to send back in a admission confirmation (ACF):

- A registered E.164 address (in this case, highly unlikely)
- A static route configured (has been observed)
- Default routing (highest frequency of problem)

## Outgoing H.323 Calls Routed to Incorrect Endpoint When Using Registration, Admissions, and Status

```
[I3 14:25:17.215 H3A3 01-1 Main] "Rel message from STACK--->H3A for callid=8, cause
code=3" [h3a_sig_sai.c:1549]
```

After the SETUP message has been sent out, a RELEASE COMPLETE is received from the remote endpoint. In this case, the remote endpoint does not service the destination address (cause code=3).

### Solution

Login to gatekeeper that outgoing H.323 gateway is registered with and determine the routing for called number. Gatekeeper could be configured to route based on several configurations:

- Called number is matched against static routing
- No routing defined for called number, uses default routing
- Routing is based on tech prefix (will be pre-pended to called number in ARQ)



## Outgoing H.323 Calls Routed to Incorrect Endpoint When Using Direct Signaling

```
[I3 14:25:17.215 H3A3 01-1 Main] "Rel message from STACK--->H3A for callid=8, cause
code=3" [h3a_sig_sai.c:1549]
```

After the SETUP message has been sent out, a RELEASE COMPLETE is received from the remote endpoint. In this case, the remote endpoint does not service the destination address (cause code=3).

Verify the value assigned to the SOFTSW\_TSAP\_ADDR for the outgoing H.323 trunk group

```
CLI>show trunk_grp id=8991;
Reply : Success: Entry 1 of 1 returned.
```

```
ID=8991
CALL_AGENT_ID=CA146
TG_TYPE=H323
SOFTSW_TSAP_ADDR=10.89.227.119;
TG_PROFILE_ID=CHINA
STATUS=INS
DIRECTION=BOTH
SEL_POLICY=ASC
GLARE=SLAVE
ALT_ROUTE_ON_CONG=N
SIGNAL_PORTED_NUMBER=N
DIAL_PLAN_ID=cdp1
DEL_DIGITS=0
OPER_STATUS=NF
```

### Solution

If the value for the SOFTSW\_TSAP\_ADDR is incorrect, use CLI to make the change as follows:

```
CLI> change trunk_grp id=8991; softsw_tsap_addr=10.89.227.219;
```

## Registration, Admissions, and Status Still Used When Outgoing H.323 Call is Provisioned to Use Direct Signaling

```
[I4 14:29:21.163 H3A3 01-1 Lib_DBM] "H3A: h3a_use_ras Checking for RAS"
[h3a_dbm.c:543]
[I4 14:29:21.163 H3A3 01-1 Lib_DBM] "H3A: we need to use the destIP from trunk_grp
table " [h3a_dbm.c:489]
[***ERROR*** 14:29:21.163 H3A3 01-1 Lib_DBM] "h3a_get_dest_ip_addr: softsw_tsap_addr
not set..." [h3a_dbm.c:494]
```

Although the configuration has specified to no use RAS, if no valid remote endpoint is provided, the fallback mechanism is to try RAS to determine the remote endpoint.

Verify the configuration for the outgoing trunk group with CLI:

```
CLI>show trunk_grp id=8991;
Reply : Success: Entry 1 of 1 returned.
```

```
ID=8991
CALL_AGENT_ID=CA146
TG_TYPE=H323
TG_PROFILE_ID=CHINA
STATUS=INS
DIRECTION=BOTH
SEL_POLICY=ASC
GLARE=SLAVE
ALT_ROUTE_ON_CONG=N
SIGNAL_PORTED_NUMBER=N
DIAL_PLAN_ID=cdp1
DEL_DIGITS=0
OPER_STATUS=NF
QOS_ID=china_qos1
TRAFFIC_TYPE=LOCAL
H323_GW_ID=CHINA_3
CAUSE_CODE_MAP_ID=H323_CHINA
ANI_BASED_ROUTING=N
NO_ANSWER_TMR=185
```

Since the SOFTSW\_TSAP\_ADDR column is not displayed, it contains a null value.

### Solution

Use CLI to change the outgoing trunk group as follows:

```
CLI> change trunk_grp id=8991; softsw_tsap_addr=10.89.227.219;
```

## Troubleshooting Integrated Services Digital Network Problems

This section describes ISDN troubleshooting and maintenance for the Cisco BTS 10200 Softswitch.

### How to Troubleshoot When the Integrated Services Digital Network Trunk Group Fails to Restore

This section shows how to troubleshoot if the ISDN trunk group fails to restore. Determine if the trunk group failed to restore by entering the following command:

```
status trunk-grp id=nnn;
```

- If the response shows Trunk group out-of-service (TG\_OOS) for the administrative state, then enter the control command.

```
status trunk-grp id=100;
```

```
Reply : Success: Entry 1 of 1 returned.
```

```
TGN_ID -100
RESULT -ADM configure result in success
REASON -ADM executed successful
ADMIN_STATE -ADMIN_OOS <=====
OPER_STATE -Trunk group out-of-service
PRIMARY_OPER_STATE -NOT USED
BACKUP_OPER_STATE -NOT USED
```

```
control trunk-grp id=nnn;mode=forced; target-state=ins;
```

- If the response does not show an operational state of *Trunk group in-service* for the trunk group (non-facility associated signaling (NFAS) or D-channel backup should also show ISDN\_DCHAN\_STATE\_INS for the D-channel operational status), then:
  - If the response is *Trunk group out-of-service*, go to Step 1.
  - If the response is *Trunk group restore session fail normal, switchover, or maint*, go to Step 2.
  - If the response is *Trunk group restore establish fail normal, switchover, or maint*, go to Step 3.
  - If the response is *ISDN\_DCHAN\_STATE\_WAIT* or *ISDN\_DCHAN\_STATE\_MB*, go to Step 4.
  - If the response is *Trunk group down session set fail hard normal, or maint*, go to Step 5.
  - If the response is *Trunk group down establish fail hard normal, or maint*, go to Step 6.
  - If the response is *Trunk group delete graceful*, go to Step 7.

---

**Step 1** Trunk group state for facility associated signaling (FAS): *Trunk group out-of-service*, or NFAS: *NFAS DCHAN\_STATE\_MOOS*.

This means the administrative state was set to in-service, but the command to go to operational state was ignored due to bad provisioning.

#### Things to Check:

Make sure that entries exist for this trunk group in the ISDN D Channel table.

**Step 2** Trunk group states for FAS: *Trunk group restore session fail normal, switchover, or maint*; or NFAS: *NFAS ISDN\_DCHAN\_STATE\_SDN*.

This means the Call Agent and the media gateway are not communicating. The backhaul session is not coming up. The problem has to do with the User Datagram Protocol (UDP) port numbers, IP addresses or domain name system (DNS) names, or network connectivity. These values are all provisioned in the Reliable User Datagram Protocol (RUDP) Backhaul Session table in the Call Agent. For Cisco IOS gateways, these values are part of the *session group groupn*....

**Things to Check:**

- a. Do the four entries in the RUDP Backhaul Session table of the Call Agent match the values in the gateway (for Cisco IOS gateways, these values are part of session group groupn...)?
- b. If the call-agent-tsap-addr, or the mgw-tsap-addr are DNS names, does **nslookup** on both Call Agents resolve the values to one unique IP address?
- c. Can the call-agent-tsap-addr in the four entries be pinged from the media gateway? Do the Call Agents actually have the IP addresses, or DNS names, specified?
- d. Can the mgw-tsap-addr be pinged from both Call Agents?
- e. Does the trunk-grp isdn-profile exist (show isdn-tg-profile ID=%)? Keep in mind that the profile ID is case sensitive.
- f. Snoop can be used to see if the gateway and Call Agent are talking in order to establish the session. Snoop can be used to eliminate whether the problem is on the Call Agent or the media gateway side.
- g. The **show backhaul session all** command on the media gateway can be useful in debugging.
- h. Look at the trace.log on the Call Agent. Search for BSM\_create\_ss or bsm\_create\_ss. This shows the exact values used by the Call Agent.



**Note** Backhaul deletion is triggered by all trunk groups of a backhaul-set being in the admin-oss state. Backhaul creation is triggered by controlling one of the trunk groups to in service (INS). The trunk group list can be determined by using the **show isdn-dchan set-id** command.

**Step 3** Trunk group states for FAS: *Trunk group restore establish fail normal, switchover, or maint* or NFAS: *ISDN\_DCHAN\_STATE\_OOS*.

This means the specific ISDN channel could not be restored. This is likely related to ISDN layer1 or layer2 not being up, or related to DCHAN-SLOT and DCHAN-PORT in the ISDN D Channel table. The media gateway and Call Agent are communicating successfully (session came up).

**Things to Check:**

- a. On the media gateway, enter a **show isdn status command**. Is Layer 1 shown as ACTIVE? If not, there may be a cable problem, or the private branch exchange (PBX) is down.
- b. Does the **show isdn status** command return a *Network side configuration*? The PBX should be set up for the user side. The gateway should be setup for the network side.
- c. Was the media gateway reloaded (rebooted) after setting up parameters? There can be problems when this has not been done. This is usually reflected by having two terminal endpoint identifier (TEI) values for the trunk level one (T1).
- d. Are the DCHAN-SLOT and DCHAN-PORT provisioned correctly in the ISDN D Channel table for this trunk group?
- e. Does the T1 on the media gateway show an alarm (red or yellow lights)? These are more clues that there is an ISDN layer1 or layer2 problem.
- f. Is the controller T1, or interface Serialn:23, provisioned correctly on the gateway?
- g. Look at the trace.log on the Call Agent. Search for BSM\_dchan\_tbl\_insert or bsm\_dchan\_tbl\_insert. The slot-port value is the actual value retrieved from the database. For the AS5300, this value should be 0, 1, 2, or 3. This is a decimal value. The top 16 bits are the slot and the bottom 16 bits are the port.

**Step 4** Trunk group states for NFAS: *ISDN\_DCHAN\_STATE\_WAIT/ISDN\_DCHAN\_STATE\_MB*.

This means the states at the far end are sending a SERVICE\_ACK to the Cisco BTS 10200 Softswitch service message for primary rate interface (PRI).

**Things to Check:**

Make sure the far end is sending a SERVICE\_ACK. There are some other trunk group states that happen after the ISDN backhaul is successfully established.

**Step 5** Trunk group states for FAS: *Trunk group down session set fail hard normal, or maint* or NFAS: *ISDN\_DCHAN\_STATE\_SDN*.

This is the same as *Trunk group restore establish request fail*, or *ISDN DChannel State SDN*. However, in this case, the D channel was already successfully established, and then went out. This likely means that the Call Agent and media gateway have lost IP connectivity. Or, the media gateway has lost power. This can also happen if the provisioning was changed, particularly the session settings in the media gateway.

**Step 6** Trunk group states for FAS: *Trunk group down establish fail hard normal, or maint* or NFAS: *NFAS ISDN\_DCHAN\_STATE\_OOS*.

This is the same as *Trunk group restore establish request fail*, or *ISDN DChannel State OOS*. However, in this case, the D channel was already successfully established, and then went out.

**Things to Check:**

- a. Is, or was, the cable unplugged between the PBX and the gateway?
- b. Was the provisioning changed on the gateway?

**Step 7** Trunk group state for FAS: *Trunk group delete graceful*.

The following command indicates you are waiting for calls to finish before going to out-of-service. If the wait time is too long, you can control the trunk group with *mode=forced*.

```
control trunk-grp id=xxxx mode=graceful target-state=oos
```

## Checking the Status of a Trunk Termination

Check the status of a trunk termination using the following command:

```
status trunk-termination tgn-id=<trunk group number>;cic=<cic number>;
```

Reply : Success:

```
RESULT -ADM configure result in success
REASON -ADM executed successful
TGN ID -2
CIC -8
TERM ADMIN STATE -ADMIN_INS
TERM OPER STATE -Termination is idle
TERM REASON -No fault reason available
TRUNK STATIC STATE -ACTV
TRUNK DYNAMIC STATE -TRNS
TRUNK REASON -NON_FAULTY
```

The above status shows that the trunk is active, in idle mode, and ready for call use.

If the trunk static state is set to locally blocked, go to the [“Trunk Static State Is Set to Locally Blocked”](#) section.

If the trunk static state is set to transient (TRNS), go to the [“Trunk Static State Is Set to Transient”](#) section.

If the trunk static state is set to remotely blocked, go to the [“Trunk Static State Is Set to Remote Block”](#) section.

If the trunk static state is set to TERM\_STATUS\_FAULTY, go to the [“Termination Status Is Faulty”](#) section.

If the trunk static state returns Cannot Make Call, go to the [“Cannot Make a Call”](#) section.

### Trunk Static State Is Set to Locally Blocked

Perform the following steps to check the *TRUNK REASON* field if the *TRUNK STATIC STATE* is set to locally blocked (LBLK) state.

- 
- Step 1** If the TRUNK REASON is set to MAINT-OOS, then a user has manually taken the trunks out of service. The user must manually put the trunks into the in-service mode.
- Use the **control** command on the specified trunk to put the trunk back into the in-service mode.
- Clear the MAINT-OOS. Trunks should be in active or idle mode and ready for use.
- Step 2** If the TRUNK REASON is set to SIGNALLING-FAULT, then the D channels are not in-service. Check the trunk group ADMIN and OPER states.
- If the trunk group ADMIN state is ADMIN\_OOS, use the **control** command to put the trunk group into in-service mode.
  - If the trunk group ADMIN state is ADMIN\_INS, verify that the trunk group OPER-STATE is IN-SERVICE (see the [How to Troubleshoot When the Integrated Services Digital Network Trunk Group Fails to Restore](#) section in case of any issues).
  - Clear any SIGNALLING-FAULT states. Trunks must be in active or idle mode and ready for use.

- Step 3** If TRUNK REASON is set to TERM\_FAULT, then the terminations are in FAULTY states. Verify the IP connectivity from the CA to the gateway.
- Clear any termination faults at the gateway by turning off, then turning on, Media Gateway Control Protocol (MGCP) (use the mgcp, no mgcp procedure on the media gateway).
  - Clear any TERM\_FAULT on the Cisco BTS 10200 Softswitch. Trunks must be in active or idle mode and ready for use.

### Trunk Static State Is Set to Transient

Perform the following steps when trunk static state is set to TRNS.



**Note**

If trunk static state is set to TRNS, then the PBX has not responded with a SERVICE\_ACK or RESTART\_ACK for the service or restart message set by the Call Agent.

- Step 1** Verify that the initialization procedure, as depicted by the associated isdn-tg-profile, and as used by PBX, is synchronized.
- Step 2** Verify that the isdn-service-supp token is set to N if PBX does not support service messages.

### Trunk Static State Is Set to Remote Block

Perform the following steps if trunk static state is set to remote block (RBLK).



**Note**

If the trunk static state is set to RBLK, and isdn-tg-profile has isdn-farend-init=Y then the PBX must start the initialization procedure, or the PBX specifically sends a service message with SERVICE-OOS mode to the Cisco BTS 10200 Softswitch to put the trunks into the remote out-of-state mode.

- Step 1** Verify that the initialization procedure (ISDN-FAREND-Initialize (INIT) token), as depicted by associated isdn-tg-profile in the Cisco BTS 10200 Softswitch, and as used by the PBX, is in sync.
- Step 2** Using the CLI command “control trunk-termination” to reset the RBLK state, perform a control trunk-termination to OOS, then control trunk-termination to INS—in case there is an error on the PBX side. Also, set the isdn-service-supp token in the ISDN trunk group profile per the procedures supported by the PBX.

### Termination Status Is Faulty

The *TERM\_STATUS\_FAULTY* message indicates an MGCP problem.

**Things to Check:**

- Is the media gateway (MGW) profile set up for the trunk?
- Is the MGW in the in-service operational state?

Perform the “no mgcp, mgcp” commands on the gateway if an MGCP problem is indicated.

## Cannot Make a Call

If you have a problem making a call, perform the following Things to Check, and then go to the [“Checking Media Gateway Provisioning” section on page 14-38](#)

### Things to Check:

When terminations are added, they have strings like S0/DS1-2/1. The S# refers to the slot number. The DS1-# refers to the port number. The /# at the end refers to the specific B channel (1–23). The slot and port numbers must match the dchan values (dchan-slot, dchan-port) for the related trunk group ID (tgn-ID), assuming that the DS0 is on a T1 that contains a D channel.

## Checking Media Gateway Provisioning

The following example shows how a Cisco IOS gateway is provisioned.



**Note** The typical problem areas are in *bold italic* type. Look at the problem area after the Call Agent is provisioned.

```
Current configuration:
!
=====
version 12.2
no service pad
service timestamps debug datetime msec
service timestamps log datetime localtime
no service password-encryption
!
hostname c2421.200
!
enable password xxxxxxxx
!
clock timezone CDT -6
network-clock base-rate 56k
network-clock-select 3 T1 0
network-clock-select 1 T1 1
network-clock-select 2 system (SCB)
IP subnet-zero
!
!
IP domain-name ipclab.cisco.com
IP name-server 10.89.224.1
!
IP audit notify log
IP audit po max-events 100
backhaul-session-manager
 set isdn1 client ft
 group group1 set isdn1
 group group2 set isdn1
 session group group1 10.89.225.223 9000 10.89.227.200 9000 1
 session group group1 10.89.226.223 9001 10.89.227.200 9001 2
 session group group2 10.89.225.224 9000 10.89.227.200 9000 1
 session group group2 10.89.226.224 9001 10.89.227.200 9001 2
isdn switch-type primary-ni
isdn voice-call-failure 0
!
!
!
```



```
!
!
!
no voice confirmation-tone
voice-card 0
!
controller T1 0
 framing esf
 linecode b8zs
 channel-group 0 timeslots 1-24 speed 64
!
controller T1 1
 framing esf
 linecode b8zs
 pri-group timeslots 1-24 service mgcp
!
!
!
!
interface Ethernet0
 IP address 10.89.227.200 255.255.255.0
 no cdp enable
!
interface Serial0
 no IP address
 shutdown
!
interface Serial0:0
 no IP address
 IP nat outside
 encapsulation ppp
 shutdown
 no cdp enable
!
interface Serial1:23
 bandwidth 64000
 no IP address
 no logging event link-status
 isdn switch-type primary-ni
 isdn protocol-emulate network
 isdn incoming-voice voice
 isdn bind-13 backhaul grp1
 no cdp enable
!
IP classless
IP route 0.0.0.0 0.0.0.0 10.89.227.254
no IP http server
IP pim bidir-enable
!
!
access-list 1 permit 10.0.24.0 0.0.0.255
call rsvp-sync
!
voice-port 1:23
!
mgcp
mgcp call-agent mgcp-SYS01CA.ipclab.cisco.com service-type mgcp version 1.0
mgcp dtmf-relay voip codec all mode nte-gw
mgcp package-capability rtp-package
mgcp default-package dt-package
no mgcp timer receive-rtcp
!
mgcp profile default
 timeout tsmx 100
```

```

max2 retries 3
!
dial-peer cor custom
!
!
!
dial-peer voice 1 pots
 application mgcpapp
 port 1:23
!
!
line con 0
line aux 0
line 2 3
line vty 0 4
 password xxxxxxxx
 login
!
ntp server 10.89.227.254
end

```

## Additional Command Line Interface Verification

Perform the following steps to provide additional CLI verification of a problem:

- 
- Step 1** Use the control command to put the trunk group out of service (OOS) and back into INS:

Place OOS:

```
control tt tgn-id=17; cic=all; target-state=oos; mode=graceful;
```

Place INS:

```
control tgn-id=17; target-state=ins; mode=forced;
```

- Step 2** If the B channel is not IDLE, use the control command to put each circuit OOS and back INS:

Place OOS:

```
control trunk-termination tgn-id=17; cic=1; target-state=oos; mode=forced;
```

Place INS:

```
control trunk-termination tgn-id=17; cic=1; target-state=ins; mode=forced;
```

- Step 3** Check the status of the trunk group:

```
status trunk-grp id=<TG ID number>; call-agent-id=<CA ID>;
```

If the trunk group status has still not changed to ADMIN\_INS—even though the commands in Steps 1 and 2 were successful—then it means that communication to the MGW has been lost. Notify your system administrator and have the problem corrected before continuing.

- Step 4** Check trunk termination and trunk status. The single command shown here queries both the trunk-termination status and trunk (channel) status:

```
status trunk-termination tgn-id=17; cic=all;

CONFIGURATION COMMAND EXECUTED TRUNK_GRP -17 -CIC -1
TERM ADMINstatus -ADMIN_INS
TERM OPERstatus -TERM_STATE_IDLE
CIC STATIC STATE -ACTV
CIC DYNAMIC STATE -IDLE

...

CONFIGURATION COMMAND EXECUTED TRUNK_GRP -17 -CIC -23
TERM ADMINstatus -ADMIN_INS
TERM OPERstatus -TERM_STATE_IDLE
CIC STATIC STATE -ACTV
CIC DYNAMIC STATE -IDLE

status trunk-termination tgn-id=17; cic=23

REPLY=CONFIGURATION COMMAND EXECUTED ISDN_TRUNK_GROUP -17 -CIC -23
TERM ADMINstatus -ADMIN_INS
TERM OPERstatus -TERM_STATE_IDLE
CIC STATIC STATE -ACTV
CIC DYNAMIC STATE -IDLE
```

## Maintenance of a Call Agent Connected to an Integrated Services Digital Network Trunk Group

During system operations, the operator can use the CLI *control* command to switch the Call Agent into one of two states:

- ACTIVE-STANDBY
- STANDBY-ACTIVE

When the control command is entered on a Call Agent connected to an ISDN trunk group (D channel), the Call Agent switchover time is approximately 20 seconds. During all but the first 6 seconds of this switchover time, the ISDN D channel is temporarily down. However, the D channel comes back up, and the ISDN trunk group automatically returns to INS, when the switchover completes.



### Note

This switchover process does not have any impact on stable calls.

# File Configuration – bts.properties

This section provides instructions for editing and configuring the bts.properties file. The default content of the the /opt/ems/etc/bts.properties file is in listed in [Table 14-1](#).

**Table 14-1**      *Default Content of the bts.properties File.*

| Parameter         | Variable                                                                                  |
|-------------------|-------------------------------------------------------------------------------------------|
| reportDir=        | /opt/ems/report                                                                           |
| reportDirSize=    | 50000000                                                                                  |
| reportSuffix=     | .html                                                                                     |
| logDefLevel=      | INFO                                                                                      |
| logMaxFileSize=   | 50000000                                                                                  |
| logMinFileSize=   | 1000                                                                                      |
| logDefFileSize=   | 4000000                                                                                   |
| logDir=           | /opt/ems/log                                                                              |
| logName=          | BtsEms                                                                                    |
| logSuffix=        | .log                                                                                      |
| logBackupSuffix=  | .bak                                                                                      |
| usersDir=         | /opt/ems/users                                                                            |
| etcDir=           | /opt/ems/etc                                                                              |
| ftpErrorsAllowed= | 3000                                                                                      |
| smgResources=     | com.sswitch.oam.smg.smg                                                                   |
| requestTimeout=   | 60000                                                                                     |
| nbsLib=           | /opt/BTSlib/lib/libnbs.so                                                                 |
| scTimeout=        | 50000                                                                                     |
| invalidChars=     | "";<br><b>Note</b> # spaces or other white space characters<br>may be considered invalid. |
| LERGDuration=     | 86400000                                                                                  |
| throttleEnable=   | N                                                                                         |

## Editing – bts.properties

Use the following instructions to edit the bts.properties file.

- Step 1

Edit the /opt/ems/etc/bts.properties file to change the desired parameter(s).
- Step 2

Shutdown and restart the affected processes.

## Example Edit – bts.properties

The following instructions for an example of how to the configure the bts.properties file to enable debugging. To enable the debugging mode and to collect the debugging information for a CLI session, use the following instruction.

- 
- Step 1** Open the /opt/ems/etc/bts.properties file.
  - Step 2** Set logDefLevel=DEBUG.  
//valid logging options are: INFO, DEBUG, ERROR, WARNING, FATAL
  - Step 3** Start a new CLI session.  
// su - btsuser
  - Step 4** Look for the log information in the /opt/ems/log/<username>.log  
// btsuser.log in this case
-





# CHAPTER 15

## Diagnostic Tests

---

Revised: October 23, 2008, OL-11335-06

### Introduction

This chapter describes diagnostic tests that can be performed on media gateways, subscriber terminations, and trunk terminations. All media gateways, subscriber and trunk terminations must be in the MAINT state for testing. The following tests are described in this section:

- [Media Gateway Tests, page 15-2](#)
- [Subscriber Termination Tests, page 15-4](#)
- [Signaling System 7 Trunk Termination Tests, page 15-6](#)
- [Integrated Services Digital Network Trunk Termination Tests, page 15-10](#)
- [Channel-Associated Signaling Trunk Termination Tests, page 15-11](#)
- [Announcement Trunk Termination Tests, page 15-13](#)
- [Troubleshooting Using Snoop, page 15-15](#)
- [Query Verification Tool and Translation Verification Tool, page 15-19](#)
- [Network Loopback Test for Network-based Call Signaling/Media Gateway Control Protocol Endpoints, page 15-30](#)
- [Session Initiation Protocol Subscriber Registration Status Check, page 15-35](#)
- [System Health Report, page 15-36](#)



#### Caution

The use of the UNIX **ifconfig down** command on any signaling interface to test or troubleshoot network or interface failures of the Cisco BTS 10200 Softswitch Signaling Interface may lead to undesirable consequences or conditions.

---

# Media Gateway Tests

This section describes the tests that can be performed on media gateways. A gateway must be in the MAINT state.

## Step 1 Force the media gateway into MAINT state:

```
control mgw id=c2421.65; mode=forced; target-state=maint;
```

Reply Example:

Reply : Success: CLI change successful

```
MGW ID -> c2421.65
INITIAL STATE -> ADMIN_INS
REQUEST STATE -> ADMIN_MAINT
RESULT STATE -> ADMIN_MAINT
FAIL REASON -> ADM found no failure
REASON -> ADM executed successful
RESULT -> ADM configure result in success
```

## Step 2 Display the Test Menu.

```
diag mgw
```

Reply Example:

```
Reply: Diagnostic MGW Menu.
===
(1) MGW Network Connectivity Test
(2) MGW MGCP Connectivity Test
(3) ALL
```



### Note

Test #1 tests if there is a path to the device (ping).  
 Test #2 tests if Media Gateway Control Protocol (MGCP) has access to the device.  
 Test #3 performs tests 1 and 2.

## Step 3 To perform a specific test, use the following examples as a guide.

```
diag mgw id=ubr-03; test=1;
```

Reply Example:

```
MEDIA GATEWAY LINE DIAGNOSTIC TEST EXECUTED -> diag mgw
ID -> ubr-03
TEST-TYPE -> ADM-MGW-NETW-CONNECTIVITY-TEST
TEST-DURATION -> 0
RESULT -> TEST-SUCCESS
REASON -> PASSED
Reply: Diagnostic command executed.
```

```
diag mgw id=ubr-03; test=2;
```

Reply Example:

```
MEDIA GATEWAY LINE DIAGNOSTIC TEST EXECUTED -> diag mgw
ID -> ubr-03
TEST-TYPE -> ADM-MGW-MGCP-CONNECTIVITY-TEST
TEST-DURATION -> 0
RESULT -> TEST-SUCCESS
REASON -> PASSED
```



Reply: Diagnostic command executed.

**diag mgw id=ubr-03; test=3;**

#### Reply Example:

```
MEDIA GATEWAY LINE DIAGNOSTIC TEST EXECUTED -> diag mgw
ID -> ubr-03
TEST-TYPE -> ADM-MGW-NETW-CONNECTIVITY-TEST
TEST-DURATION -> 11
RESULT -> TEST-SUCCESS
REASON -> PASSED
```

```
MEDIA GATEWAY LINE DIAGNOSTIC TEST EXECUTED -> diag mgw
ID -> ubr-03
TEST-TYPE -> ADM-MGW-MGCP-CONNECTIVITY-TEST
TEST-DURATION -> 0
RESULT -> TEST-SUCCESS
REASON -> PASSED
Reply: Diagnostic command executed.
```

#### Step 4 Force the media gateway into INS state:

**control mgw id=c2421.65; mode=forced; target-state=ins;**

#### Reply Example:

Reply : Success: CLI change successful

```
MGW ID -> c2421.65
INITIAL STATE -> ADMIN_MAINT
REQUEST STATE -> ADMIN_INS
RESULT STATE -> ADMIN_INS
FAIL REASON -> ADM found no failure
REASON -> ADM executed successful
RESULT -> ADM configure result in success
```

---

# Subscriber Termination Tests

This section describes the tests that can be performed on subscriber terminations. All terminations must be in the MAINT state.

**Step 1** Force the subscriber termination into MAINT state:

```
control subscriber-termination id=sub2-ctx2; mode=forced; target-state=maint;
```

**Step 2** Display the Test Menu.

```
diag subscriber-termination;
```

Reply Example:

```
Reply: Diagnostic Subscriber Menu.
===
(1) Subscriber MGCP Connectivity Test
(2) Subscriber Termination Connection Test
(3) Subscriber Termination Ring Test
(4) ALL
```



## Note

Test #1 tests if MGCP has access to the termination.

Test #2 tests if there is a path to the device (ping).

Test #3 tests if the subscriber can be rung. The Ring parameter must be specified in seconds for this test. The default is 5 seconds.

Test #4 performs tests 1 through 3.

**Step 3** To perform a specific test, use the following examples as a guide.

```
diag subscriber-termination id=sub2-ctx2; test=1;
```

Reply Example:

```
SUBSCRIBER LINE DIAGNOSTIC TEST EXECUTED -> diag subscriber-termination
ID -> sub2-ctx2
TEST-TYPE -> ADM-MGW-MGCP-CONNECTIVITY-TEST
TEST-DURATION -> 10
RESULT -> TEST-SUCCESS
REASON -> PASSED: Reason: AUEP-NACK received with RespCode = 510
Reply: Diagnostic command executed.
```

```
diag subscriber-termination id=sub-ubr3-1@cisco.com; test=2;
```

Reply Example:

```
SUBSCRIBER LINE DIAGNOSTIC TEST EXECUTED -> diag subscriber-termination
ID -> sub-ubr3-1@Cisco.com
TEST-TYPE -> ADM-TERM-CONNECTION-TEST
TEST-DURATION -> 55
RESULT -> TEST-SUCCESS
REASON -> PASS successfully.
Reply: Diagnostic command executed.
```

```
diag subscriber-termination id=sub-ubr3-1@cisco.com; test=3; ring-duration=10;
```

Reply Example:

```
SUBSCRIBER LINE DIAGNOSTIC TEST EXECUTED -> diag subscriber-termination
ID -> sub-ubr3-1@Cisco.com
TEST-TYPE -> ADM-TERM-RING-TEST
```

```
TEST-DURATION -> 9989
RESULT -> TEST-SUCCESS
REASON -> PASSED
Reply: Diagnostic command executed.
```

**Step 4** Force the subscriber termination into INS state:

```
control subscriber-termination id=sub2-ctx2; mode=forced; target-state=ins;
```



**Note**

Ring-duration values are 0–999 (Default = 5). Maximum ring time is 30 seconds regardless of whether the duration is set higher than or equal to 31.

# Signaling System 7 Trunk Termination Tests

This section describes the tests that can be performed on Signaling System 7 (SS7) trunk terminations. All terminations must be in the MAINT state for testing.

**Step 1** Force the SS7 trunk termination into MAINT state:

```
control ss7-trunk-termination tgn-id=103; mode=forced; target-state=maint;
```



**Note** Set customer-originated trace (COT), circuit verification message (CVM), and circuit query message (CQM) on the terminating gateway or switch to perform these tests. Otherwise, the test or tests will fail.

**Step 2** Display the Test Menu.

```
diag ss7-trunk-termination
```

Reply Example:

```
Reply: Diagnostic SS7 Trunk Group Menu.
===
Test=1: SS7 MGCP Connectivity
Test=2: SS7 Termination Connection Test
Test=3: COT
Test=4: CQM
Test=5: CVT
Test=6: CIC
Test=7: All
```



**Note** Test #1 tests if MGCP has access to the SS7 trunk termination.  
 Test #2 tests if there is a path to the device (ping).  
 Test #3 tests the integrity of the SS7 Bearer Path.  
 Test #4 queries the SS7 circuit (or group of circuits) status. A range of CICs can be specified (to a maximum of 24). Both remote and local trunk states are displayed in the results.  
 Test #5 tests to ensure that each end of the circuit has sufficient and consistent information for using the circuit in call connections. Common language location identifier (CLLI) names are included.  
 Test #6 tests to ensure the CIC connections.  
 Test #7 performs tests 1 through 6.

**Step 3** To perform a specific test, use the following examples as a guide:

```
diag ss7-trunk-termination tgn-id=103; cic=13; test=1;
```

Reply Example:

```
TRUNK DIAGNOSTIC TEST EXECUTED -> diag trunk
TG-NUM -> 103
CIC -> 13
TEST-TYPE -> ADM-MGW-MGCP-CONNECTIVITY-TEST
TEST-DURATION -> 0
RESULT -> TEST-SUCCESS
REASON -> PASSED: Reason: AUEP-NACK received with RespCode = 510
Reply: Diagnostic command executed.
```

```
diag ss7-trunk-termination tgn-id=103; cic=13; test=2;
```

**Reply Example:**

```
TRUNK DIAGNOSTIC TEST EXECUTED -> diag trunk
TG-NUM -> 103
CIC -> 13
TEST-TYPE -> ADM-TERM-CONNECTION-TEST
TEST-DURATION -> 33
RESULT -> TEST-SUCCESS
REASON -> PASS successfully.
Reply: Diagnostic command executed.
```

**diag ss7-trunk-termination tgn-id=103; cic=14; test=3;**

**Reply Example:**

```
TRUNK DIAGNOSTIC TEST EXECUTED -> diag trunk
TG-NUM -> 103
CIC -> 14
TEST-TYPE -> ADM-SS7-COT-TEST
TEST-DURATION -> 0
RESULT -> TEST-FAILURE
REASON -> ADM-MAINT-STATE-REQUIRED
Reply: Diagnostic command executed.
```

**diag ss7-trunk-termination tgn-id=2;cic=1-24;test=4**

**Reply Example:**

Reply : Success:

```
TGN ID -> 2
START CIC -> 1
END CIC -> 24
TEST TYPE -> ADM running SS7 circuit query message test
TEST DURATION -> 0
RESULT -> ADM ran test successfully
REASON -> CQM test pass
CIC COUNT -> 24
CIC STATES ->
```

| Remote State      | Local State |
|-------------------|-------------|
| CIC 1 -> CS_IDLE  | ACTV IDLE   |
| CIC 2 -> CS_IDLE  | ACTV IDLE   |
| CIC 3 -> CS_IDLE  | ACTV IDLE   |
| CIC 4 -> CS_IDLE  | ACTV IDLE   |
| CIC 5 -> CS_IDLE  | ACTV IDLE   |
| CIC 6 -> CS_IDLE  | ACTV IDLE   |
| CIC 7 -> CS_IDLE  | ACTV IDLE   |
| CIC 8 -> CS_IDLE  | ACTV IDLE   |
| CIC 9 -> CS_IDLE  | ACTV IDLE   |
| CIC 10 -> CS_IDLE | ACTV IDLE   |

```

CIC 11 -> CS_IDLE ACTV IDLE
CIC 12 -> CS_IDLE ACTV IDLE
CIC 13 -> CS_IDLE ACTV IDLE
CIC 14 -> CS_IDLE ACTV IDLE
CIC 15 -> CS_IDLE ACTV IDLE
CIC 16 -> CS_IDLE ACTV IDLE
CIC 17 -> CS_IDLE ACTV IDLE
CIC 18 -> CS_IDLE ACTV IDLE
CIC 19 -> CS_IDLE ACTV IDLE
CIC 20 -> CS_IDLE ACTV IDLE
CIC 21 -> CS_IDLE ACTV IDLE
CIC 22 -> CS_IDLE ACTV IDLE
CIC 23 -> CS_IDLE ACTV IDLE
CIC 24 -> CS_IDLE ACTV IDLE

```

**Note**

[Table 15-1](#) lists the responses that can be returned for the CQM test:

```
diag ss7-trunk-termination tgn-id=2;cic=1;test=5
```

**Reply Example:**

Reply : Success:

```

TGN ID -> 2
START CIC -> 1
END CIC -> 1
TEST TYPE -> ADM running SS7 circuit validation test
TEST DURATION -> 0
RESULT -> ADM ran test successfully
REASON -> CVT test pass
CLLI -> DALLTXRCDN5

```

**Step 4** Force the SS7 trunk termination into INS state:

```
control ss7-trunk-termination tgn-id=103; mode=forced; target-state=ins;
```

**Table 15-1**      **CQM Responses**

| <b>Response</b>         | <b>Description</b>                                                         |
|-------------------------|----------------------------------------------------------------------------|
| CS_TRANSIENT            | Transient                                                                  |
| CS_UNEQUIPPED           | Unequipped                                                                 |
| CS_IC_BUSY              | Incoming Busy                                                              |
| CS_IC_BUSY_LOCBLOC      | Incoming Busy and Locally Maintenance Blocked                              |
| CS_IC_BUSY_REMBLOC      | Incoming Busy and Remotely Maintenance Blocked                             |
| CS_IC_BUSY_BOTH_BLOC    | Incoming Busy and Remotely and Locally Maintenance Blocked                 |
| CS_OG_BUSY              | Outgoing Busy                                                              |
| CS_OG_BUSY_LOCBLOC      | Outgoing Busy and Locally Maintenance Blocked                              |
| CS_OG_BUSY_REMBLOC      | Outgoing Busy and Remotely Maintenance Blocked                             |
| CS_OG_BUSY_BOTH_BLOC    | Outgoing Busy and Remotely and Locally Maintenance Blocked                 |
| CS_IDLE                 | Idle                                                                       |
| CS_IDLE_LOCBLOC         | Idle and Locally Maintenance Blocked                                       |
| CS_IDLE_REMBLOC         | Idle and remotely maintenance blocked                                      |
| CS_IDLE_BOTH_BLOC       | Idle and Remotely and Locally Maintenance Blocked                          |
| CS_HW_LOCBLOC           | Locally Hardware Blocked                                                   |
| CS_HW_LOCBLOC_LOCBLOC   | Locally Hardware and Locally Maintenance Blocked                           |
| CS_HW_LOCBLOC_REMBLOC   | Locally Hardware and Remotely Maintenance Blocked                          |
| CS_HW_LOCBLOC_BOTHBLOC  | Locally Hardware and Remotely and Locally Maintenance Blocked              |
| CS_HW_REMBLOC           | Remotely Hardware Blocked                                                  |
| CS_HW_REMBLOC_LOCBLOC   | Remotely Hardware and Locally Maintenance Blocked                          |
| CS_HW_REMBLOC_REMBLOC   | Remotely Hardware and Remotely Maintenance Blocked                         |
| CS_HW_REMBLOC_BOTHBLOC  | Remotely Hardware and Remotely and Locally Maintenance Blocked             |
| CS_HW_BOTHBLOC          | Remotely and Locally Hardware Blocked                                      |
| CS_HW_BOTHBLOC_LOCBLOC  | Remotely and Locally Hardware and Locally Maintenance Blocked              |
| CS_HW_BOTHBLOC_REMBLOC  | Remotely and Locally Hardware and Remotely Maintenance Blocked             |
| CS_HW_BOTHBLOC_BOTHBLOC | Remotely and Locally Hardware and Remotely and Locally Maintenance Blocked |

# Integrated Services Digital Network Trunk Termination Tests

This section describes the tests that can be performed on Integrated Services Digital Network (ISDN) trunk terminations. All terminations must be in the MAINT state for testing.

**Step 1** Force the ISDN trunk termination into MAINT state:

```
control isdn-trunk-termination tgn-id=17; mode=forced; target-state=maint;
```

**Step 2** Display the Test Menu.

```
diag isdn-trunk-termination
```

Reply Example:

```
Reply: Diagnostic ISDN Trunk Group Menu.
===
(1) ISDN MGCP Connectivity Test
(2) ISDN Termination Connection Test
(3) ALL
```



**Note**

Test #1 tests if MGCP has access to the ISDN termination.  
Test #2 tests if there is a path to the device (ping).  
Test #3 performs tests 1 and 2.

**Step 3** To perform a specific test, use the following examples as a guide.

```
diag isdn-trunk-termination test=1; tgn-id=17; cic=1;
```

Reply Example:

```
TRUNK DIAGNOSTIC TEST EXECUTED -> diag trunk
TG-NUM -> 17
CIC -> 1
TEST-TYPE -> ADM-MGW-MGCP-CONNECTIVITY-TEST
TEST-DURATION -> 0
RESULT -> TEST-SUCCESS
REASON -> PASSED: Reason: AUEP-NACK received with RespCode = 510
Reply: Diagnostic command executed.
```

```
diag isdn-trunk-termination test=2; tgn-id=17; cic=1;
```

Reply Example:

```
TRUNK DIAGNOSTIC TEST EXECUTED -> diag trunk
TG-NUM -> 17
CIC -> 1
TEST-TYPE -> ADM-TERM-CONNECTION-TEST
TEST-DURATION -> 0
RESULT -> TEST-SUCCESS
REASON -> PASSED: Reason: AUEP-NACK received with RespCode = 510
Reply: Diagnostic command executed.
```

**Step 4** Force the ISDN trunk termination into MAINT state:

```
control isdn-trunk-termination tgn-id=17; mode=forced; target-state=maint;
```



# Channel-Associated Signaling Trunk Termination Tests

This section describes the tests that can be performed on channel-associated signaling (CAS) trunk terminations. All terminations must be in the MAINT state for testing.

**Step 1** Force the CAS trunk termination into MAINT state:

```
control cas-trunk-termination tgn-id=64; mode=forced; target-state=maint;
```

**Step 2** Display the Test Menu.

```
diag cas-trunk-termination
```

Reply Example:

Reply: Diagnostic CAS Trunk Group Menu.

===

(1) CAS MGCP Connectivity Test

(2) CAS Termination Connection Test

(3) ALL



**Note**

Test #1 tests if MGCP has access to the CAS termination.

Test #2 tests if there is a path to the device (ping).

Test #3 performs tests 1 and 2.

**Step 3** To perform a specific test, use the following examples as a guide:

```
diag cas-trunk-termination tgn-id=64;cic=1;test=1;
```

Reply Example:

TRUNK DIAGNOSTIC TEST EXECUTED -> diag trunk

TG-NUM -> 64

CIC -> 1

TEST-TYPE -> ADM-MGW-MGCP-CONNECTIVITY-TEST

TEST-DURATION -> 0

RESULT -> TEST-SUCCESS

REASON -> PASSED: Reason: AUEP-NACK received with RespCode = 510

Reply: Diagnostic command executed.

```
diag cas-trunk-termination tgn-id=64;cic=1;test=2;
```

Reply Example:

TRUNK DIAGNOSTIC TEST EXECUTED -> diag trunk

TG-NUM -> 64

CIC -> 1

TEST-TYPE -> ADM-TERM-CONNECTION-TEST

TEST-DURATION -> 32

RESULT -> TEST-SUCCESS

REASON -> PASS successfully.

Reply: Diagnostic command executed.

```
diag cas-trunk-termination tgn-id=64;cic=1;test=3;
```

Reply Example:

TRUNK DIAGNOSTIC TEST EXECUTED -> diag trunk

TG-NUM -> 64

CIC -> 1

TEST-TYPE -> ADM-MGW-MGCP-CONNECTIVITY-TEST

TEST-DURATION -> 11

```
RESULT -> TEST-SUCCESS
REASON -> PASSED: Reason: AUEP-NACK received with RespCode = 510

TRUNK DIAGNOSTIC TEST EXECUTED -> diag trunk
TG-NUM -> 64
CIC -> 1
TEST-TYPE -> ADM-TERM-CONNECTION-TEST
TEST-DURATION -> 32
RESULT -> TEST-SUCCESS
REASON -> PASS successfully.
Reply: Diagnostic command executed.
```

**Step 4** Force the CAS trunk termination into INS state:

```
control cas-trunk-termination tgn-id=64; mode=forced; target-state=ins;
```

---

# Announcement Trunk Termination Tests

This section describes the tests that can be performed on Announcement trunk terminations. All terminations must be in the MAINT state for testing.

**Step 1** Force the Announcement trunk termination into MAINT state:

```
control annnc-trunk-termination tgn-id=13; mode=forced; target-state=maint;
```

**Step 2** Display the Test Menu.

```
diag annnc-trunk-termination:
```

Reply Example:

```
Reply: Diagnostic ANC Trunk Group Menu.
===
(1) ANC MGCP Connectivity Test
(2) ANC Termination Connection Test
(3) ALL
```



## Note

Test #1 tests if MGCP has access to the announcements module (ANC) termination.  
Test #2, tests if there is a path to the device (ping).  
Test #3 performs tests 1 and 2.

**Step 3** To perform a specific test, use the following examples as a guide.

```
diag annnc-trunk-termination;test=1;tgn-id=13;cic=1
```

Reply Example:

```
TRUNK DIAGNOSTIC TEST EXECUTED -> diag trunk
TG-NUM -> 13
CIC -> 1
TEST-TYPE -> ADM-MGW-MGCP-CONNECTIVITY-TEST
TEST-DURATION -> 0
RESULT -> TEST-SUCCESS
REASON -> PASSED: Reason: AUEP-NACK received with RespCode = 510
Reply: Diagnostic command executed.
```

```
diag annnc-trunk-termination;test=2;tgn-id=13;cic=1
```

Reply Example:

```
TRUNK DIAGNOSTIC TEST EXECUTED -> diag trunk
TG-NUM -> 13
CIC -> 1
TEST-TYPE -> ADM-TERM-CONNECTION-TEST
TEST-DURATION -> 33
RESULT -> TEST-SUCCESS
REASON -> PASS successfully.
Reply: Diagnostic command executed.
```

```
diag annnc-trunk-termination;test=3;tgn-id=13;cic=1
```

Reply Example:

```
TRUNK DIAGNOSTIC TEST EXECUTED -> diag trunk
TG-NUM -> 13
CIC -> 1
TEST-TYPE -> ADM-MGW-MGCP-CONNECTIVITY-TEST
```

```
TEST-DURATION -> 11
RESULT -> TEST-SUCCESS
REASON -> PASSED: Reason: AUEP-NACK received with RespCode = 510

TRUNK DIAGNOSTIC TEST EXECUTED -> diag trunk
TG-NUM -> 13
CIC -> 1
TEST-TYPE -> ADM-TERM-CONNECTION-TEST
TEST-DURATION -> 33
RESULT -> TEST-SUCCESS
REASON -> PASS successfully.
Reply: Diagnostic command executed.
```

**Step 4** Force the Announcement trunk termination into INS state:

```
control annnc-trunk-termination tgn-id=13; mode=forced; target-state=ins;
```

---

# Troubleshooting Using Snoop



## Caution

Snoop should NOT be used on the Cisco BTS 10200 Softswitch call agent itself in a Production Network. It can cause performance degradation.

Snoop can be used on the Cisco BTS 10200 Softswitch call agent during test and turn-up phase during very low call volume periods. Snoop can always be used on a separate UNIX machine connected to a switch that has been properly setup for port span/mirroring. You must be logged in as “root” user to run snoop. Snoop can be used to decode text protocols or can be saved to a file and opened with Ethereal when binary protocols are used. Ethereal is open source software and can be downloaded from <http://www.ethereal.com>. To use Snoop to diagnose network problems, take the following steps:

## Step 1

Find all routes to the destination in question. Most likely there will be multiple routes therefore multiple interfaces will need to be snooped. (Skip this step if you are snooping from a separate Unix machine - you will just snoop the span destination interface in that case.) In this example, destination Internet Protocol (IP) 10.0.0.1 is in question. The fully qualified domain name (FQDN) can be used if it is resolvable by domain name system (DNS). Issue the command several times as there may be redundant routes.

```
mssol-ca0-a# route get 10.0.0.1
 route to: 10.0.0.1
destination: default
 mask: default
 gateway: 10.0.0.253
 interface: qfe4
 flags: <UP,GATEWAY,DONE>
 rcvpipe sendpipe ssthresh rtt,ms rttvar,ms hopcount mtu expire
 0 0 0 0 0 0 1500 0
mssol-ca0-a# route get 10.0.0.1
 route to: 10.0.0.1
destination: default
 mask: default
 gateway: 10.0.0.253
 interface: qfe4
 flags: <UP,GATEWAY,DONE>
 rcvpipe sendpipe ssthresh rtt,ms rttvar,ms hopcount mtu expire
 0 0 0 0 0 0 1500 0
mssol-ca0-a# route get 10.0.0.1
 route to: 10.0.0.1
destination: default
 mask: default
 gateway: 10.20.0.253
 interface: qfe0
 flags: <UP,GATEWAY,DONE>
 rcvpipe sendpipe ssthresh rtt,ms rttvar,ms hopcount mtu expire
 0 0 0 0 0 0 1500 0
mssol-ca0-a# route get 10.0.0.1
 route to: 10.0.0.1
destination: default
 mask: default
 gateway: 10.20.0.253
 interface: qfe0
 flags: <UP,GATEWAY,DONE>
 rcvpipe sendpipe ssthresh rtt,ms rttvar,ms hopcount mtu expire
 0 0 0 0 0 0 1500 0
```

**Note**

Each interface reported above must be snooped to catch all packets across redundant routes. In the given example interface qfe0 as well as qfe4 must be snooped.

**Step 2** Issue the snoop command. It may differ in syntax depending on protocol(s) that are being analyzed.

Session Initiation Protocol (SIP) example:

10.0.0.1 is a SIP Phone. The goal is to monitor the SIP traffic between the Cisco BTS 10200 Softswitch and the SIP phone.

```
snoop -d qfe0 -x 42 host 10.0.0.1 and port 5060 and udp &
snoop -d qfe4 -x 42 host 10.0.0.1 and port 5060 and udp &
```

MGCP/network-based call signaling (NCS) example:

10.0.0.1 is an integrated access device (IAD) running MGCP. The goal is to monitor MGCP traffic between the Cisco BTS 10200 Softswitch and the IAD.

```
snoop -d qfe0 -x 42 host 10.0.0.1 and port 2427 and udp &
snoop -d qfe4 -x 42 host 10.0.0.1 and port 2427 and udp &
```

Stream Control Transmission Protocol (SCTP)/MTP3 user adaptation (M3UA)/ISDN user part (ISUP) example:

Since these protocols are not TEXT based as the ones mentioned above, use the -o option with snoop to capture packets in an Ethereal readable format. Ethereal can decode SCTP/M3UA/ISUP or SCTP/SCCP user adapter (SUA)/Transaction Capabilities Application Part (TCAP). 10.0.0.1 is a Signaling Gateway acting as an M3UA peer with the Cisco BTS 10200 Softswitch.

```
snoop -d qfe0 -o sctp.cap host 10.0.0.1 (this will capture all traffic)
```

**Step 3** Use Control-C to stop the packet capture. Open the file in Ethereal and inspect. To capture sctp packets that contain M3UA information:

**a.** First, find the port M3UA will use to communicate with the signaling gateway (SG).

```
CLI>show sctp-assoc platform-id=CA146

ID=sgp1-itpa
SGP_ID=sgp1
SCTP_ASSOC_PROFILE_ID=sctp-prof1
REMOTE_PORT=2905 <-----this port
REMOTE_TSAP_ADDR1=10.0.0.1
PLATFORM_ID=CA146
DSCP=NONE
IP_TOS_PRECEDENCE=CRITICAL
LOCAL_RCVWIN=3000
MAX_INIT_RETRANS=3
MAX_INIT_RTO=500
STATUS=INS
ULP=XUA

snoop -d qfe0 -o m3ua.cap host 10.0.0.1 and port 2905
```

**b.** Use Control-C to stop the packet capture. Open the file in Ethereal and inspect.

SCTP/SUA/TCAP example 1:

10.0.0.1 is a Signaling Gateway acting as an SUA peer with the Cisco BTS 10200 Softswitch. The goal is to capture all 800/local number portability (LNP) queries.

**a.** Follow the same syntax as for the M3UA case, except find which port SUA communicates with the SG for Advanced Intelligent Network (AIN) features:

```

CLI>show sctp-assoc platform-id=FSAIN205

ID=sctp-ain-itypa
SGP_ID=sgp1
SCTP_ASSOC_PROFILE_ID=sctp-profl
REMOTE_PORT=2907 <-----this port
REMOTE_TSAP_ADDR1=10.0.0.1
PLATFORM_ID=FSAIN205
DSCP=NONE
IP_TOS_PRECEDENCE=CRITICAL
LOCAL_RCVWIN=3000
MAX_INIT_RETRANS=3
MAX_INIT_RTO=500
STATUS=INS
ULP=XUA

snoop -d qfe0 -o suaain.cap host 10.0.0.1 and port 2907

```

- b.** Use Control-C to stop the packet capture. Open the file in Ethereal and inspect.

#### SCTP/SUA/TCAP example 2:

10.0.0.1 is a Signaling Gateway acting as an SUA peer with the Cisco BTS 10200 Softswitch. The goal is to capture all offnet automatic callback and automatic rollback (ACAR) queries.

- a.** Follow the same syntax as for the M3UA case, except find the port SUA communicates with the SG for plain old telephone service (POTS) features:

```

CLI>show sctp-assoc platform-id=FSPTC235

ID=sctp-ptc-itypa
SGP_ID=sgp2
SCTP_ASSOC_PROFILE_ID=sctp-profl
REMOTE_PORT=2906 <-----this port
REMOTE_TSAP_ADDR1=10.0.0.1
PLATFORM_ID=FSPTC235
DSCP=NONE
IP_TOS_PRECEDENCE=FLASH
LOCAL_RCVWIN=64000
MAX_INIT_RETRANS=5
MAX_INIT_RTO=1000
STATUS=INS
ULP=XUA

snoop -d qfe0 -o suapots.cap host 10.0.0.1 and port 2906

```

- b.** Use Control-C to stop the packet capture. Open the file in Ethereal and inspect.

#### H.323 Protocol (H323) example:

10.0.0.1 is an H323 gateway. 10.0.0.129 is an H323 gatekeeper. Our goal is to monitor both Registration, Admissions, and Status (RAS) and H.225 messaging.

- a.** First, find the RAS port number and the H.225 port number.

```

CLI>show h323-gw

ID=ccm3_gw1
STATUS=INS
OPER_STATUS=NF
GW_H225_PORT=1720 <----- this port
TGN_ID=4441
SECURITY=N
H245_TUNNELING=DEFAULT
TCP_MAX_LIMIT=5

```

```

TCP_MAX_AGE=30
MAX_VOIP_CALLS=65535
HIGH_WATER_MARK=0
LOW_WATER_MARK=0
IRR_BANDWIDTH_SUPP=N
IPTOS_SIG_LOWDELAY=Y
IPTOS_SIG_THROUGHPUT=N
IPTOS_SIG_RELIABILITY=N
IPTOS_SIG_PRECEDENCE=FLASH
BRQ_SUPP=Y
ANNEXE_RETRANSMIT_TIMER=500
ANNEXE_RETRANSMIT_MULTIPLIER=2
ANNEXE_RETRANSMIT_ATTEMPTS=8
CALL_START_MODE=FAST_START
ANNEXE_SUPP=N
ANNEXR_SUPP=N
STATUS_ENQ_TIMER=4
CODEC_NEG_TIMER=200
CODEC_NEG_ATTEMPTS=4
SOURCE_BASED_ROUTING=NONE

CLI>show h323-gw2gk

H323_GW_ID=ccm3_gw1
GK_ID=Metro-GK
PRIORITY=0
GK_IP_ADDR=10.0.0.129
GK_RAS_PORT=1719 <----- this port
MULTICAST=N
TIME_TO_LIVE=60

snoop -d qfe0 -o h323.cap host 10.0.0.1 and port 1720 or host 10.0.0.129 and port
1719

```

- b.** Use Control-C to stop the packet capture. Open the file in Ethereal and inspect.

COPs example:

10.0.0.1 is a cable modem termination system (CMTS) and is configured as an aggregation identification (AGGR-ID) in the Cisco BTS 10200 Softswitch. The goal is to monitor all Common Open Policy Service Protocol (COPS) messaging to and from the CMTS.

- a.** Issue the following command:

```
snoop -d qfe0 -o cops.cap host 10.0.0.1 and port 2126 and tcp
```

- b.** Use Control-C to stop the packet capture. Open the file in Ethereal and inspect.

**Step 4** Packets can be redirected to a file (not readable by Ethereal) at follows:

```
snoop -d qfe0 -x 42 host 10.0.0.1 and port 2427 and udp > mycapt.cap
```

**Step 5** Stop the snoop processes.

```
pkill snoop
pgrep snoop (should not report any process ids)
```

---



# Query Verification Tool and Translation Verification Tool

This section describes the Query Verification Tool (QVT) and the Translation Verification Tool (TVT) and is organized into the following sub-sections:

- [Tool Requirements, page 15-19](#)
- [Query Verification Tool, page 15-19](#)
- [Translation Verification Tool, page 15-26](#)
- [Using Query Verification Tool and Translation Verification Tool Together, page 15-28](#)

## Tool Requirements

The following requirements are supported in the QVT and TVT:

- TVT—Provide a tool to find, diagnose, and trace call flow path decisions.
- Query Local Routing Number (QLRN) Tool—Provide the ability to enter a ten digit directory number and launch a query to the service control point (SCP) as though it was a called number from the signal switching point (SSP).
- Query Tool E800VER Command—Send a database query to the SCP as if it was an 800 called number from the SSP without initiating a call.
- Query Tool CNAMDVER and TESTSS CNAMD Commands—Provide the ability to query the SCP database for the calling name delivery (CNAM) display and privacy status associated with the name without initiating a call.

## Query Verification Tool

This section describes the QVT and includes the following sections:

- [Overview, page 15-19](#)
- [Command Format, page 15-20](#)
- [Response Format, page 15-21](#)
- [Query Errors, page 15-22](#)
- [Query Verification Tool Measurements, page 15-26](#)

## Overview

The QVT enables a user to generate TCAP queries to external databases through the command line interface (CLI) interface. The types of queries supported are:

- Line information database (LIDB)—Generated by the POTS Feature Server
- Toll-Free—Generated by the AIN Feature Server
- LNP—Generated by the AIN Feature Server

## Command Format

The QVT command uses the following format:

```
query <lidb|toll-free|lnp> parameter=value;
```

### Examples

```
query lidb calling-dn=8002550002; opc-id=opc;
```

### Syntax Description

|              |                                                                                                        |
|--------------|--------------------------------------------------------------------------------------------------------|
| * OPC-Id     | Origination Point Code ID                                                                              |
| * Calling-DN | The caller's directory number.                                                                         |
| Table-Info   | Specifies whether or not you want to see the tables accessed when processing the query. Y/N; default=N |

### Examples

```
query toll-free
```

### Syntax Description

|                                    |                                                                                                                                                                 |
|------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| * OPC-Id                           | Origination Point Code ID                                                                                                                                       |
| * Calling-DN                       | The caller's directory number.                                                                                                                                  |
| * User-Type                        | Specifies whether the User-ID is a Trunk-Group-ID or the Calling-DN. Mandatory for AIN0.1 queries; not used in intelligent network (IN)/I queries.              |
| * User-ID                          | Specifies either the Trunk-Group-ID or Calling-DN, depending upon what you have specified in User-Type. Mandatory for AIN0.1 queries; not used in IN/I queries. |
| * Called-DN                        |                                                                                                                                                                 |
| * LATA                             | Local access and transport area. VARCHAR (5)                                                                                                                    |
| Originating Line Information (OLI) | Optional parameter used if the message-type is IN/I. 0 (default) = POTS.                                                                                        |
| Bearer-Capability                  | Valid values are: Speech, f31KhzAudio, b56kbps, or b64kbps.                                                                                                     |
| Trigger-Criteria                   | Valid values are: 3, 6, 7, 8, 9, or 10.                                                                                                                         |
| Table-Info                         | Specifies whether or not you want to see the tables accessed when processing the query. Y/N; default=N                                                          |

### Examples

```
query lnp;
```

|                           |                   |                                                                                                                                                                                                             |
|---------------------------|-------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax Description</b> | * OPC-Id          | Origination Point Code ID                                                                                                                                                                                   |
|                           | * Calling-DN      | The caller's directory number. VARCHAR(10): 10 digits in the format npaxxxxxxx.                                                                                                                             |
|                           | * User-Type       | Specifies whether the User-ID is a Trunk-Group-ID or the Calling-DN.                                                                                                                                        |
|                           | * User-ID         | Specifies either the Trunk-Group-ID or Calling-DN, depending upon what you have specified in User-Type. Values are POTS DN NPA-NXX-XXXX (Calling-DN) or numeric number nomenclature (NNN) (Trunk-Group-ID). |
|                           | * Called-DN       |                                                                                                                                                                                                             |
|                           | * LATA            | Local access and transport area. VARCHAR (5)                                                                                                                                                                |
|                           | Bearer-Capability | Valid values are: Speech, f31KhzAudio, b56kbps, or b64kbps.                                                                                                                                                 |
|                           | Trigger-Criteria  |                                                                                                                                                                                                             |
|                           | Table-Info        | Specifies whether or not you want to see the tables accessed when processing the query. Y/N; default=N                                                                                                      |

## Response Format

The system response to a query is in the following format:

Reply: <success|failure>; parameter=value;

### Common Response Parameters

Successful response parameters include the following:

- OPC—Originating Point Code
- SSN—Subsystem Number
- TT—translation type
- SCP-Point-Code—Point Code of the SCP
- Automatic call gapping (ACG) component received
- ACG-Control-Code-Length
- Generic address parameter (GAP) – duration
- GAP-Interval
- Announcement-Cause-Code

An error message will be displayed if the query is not successful. For more information about error messages and problem resolution, refer to the “Query Errors” section on page 4.

### Query Line Information Database Response Parameters

Additional parameters returned in response to a query lidb command include:

- Calling-DN
- Caller-ID Name String
- Caller-ID Name Privacy

## Query Toll-Free Parameters

The following additional parameters are returned in response to a query toll-free command:

- Message-Type
- Original Number
- Translated Number
- Carrier
- Send-Notification-Received

## Query Local Number Portability Parameters

The following additional parameters are returned in response to a query LNP command:

- Original Number
- Translated Number

## Query Errors

An error can occur when a query command fails. This section specifies error responses and possible resolutions for problems.

### Request Timeout

A query is sent to the feature server, but no response is received. The error response is similar to the following example:

```
CLI> query lldb; calling-dn=123247238723; opc-id=opc;
QUERY ON FEATURE SERVER FSPTC235 IS ...->
FSPTC235 -> No Reply received!
Reply : Failure:
CLI>
```

The Feature Server did not respond to the query before a timeout occurred. Take the following steps to resolve the problem:

- If it was an LIDB query, execute the nodestat command on the POTS Feature Server to confirm that it is Active.
- If it was a Toll-Free or LNP query, execute the nodestat command on the AIN Feature Server to confirm that it is Active.
- If the platform is Active, execute the following command to confirm that the selective call acceptance (SCA) process is running:

```
ps -aef | grep sca
```

If the process is not running, start it through process debug manager (PDM) or by stopping and restarting the platform.

- If the platform is Active, execute the following command to confirm that the TCAP signaling adapter (TSA) process is running:

```
ps -aef | grep tsa
```

If the process is not running, start it through PDM or by stopping and restarting the platform.

- If the SCA and TSA processes are running on the Active platform, check the trace files for errors associated with the query.

## Service Control Point Timeout

The SCP does not respond to a query. The error response is similar to the following example:

```
CLI> query lldb; calling-dn=1232472387283; opc-id=opc;
QUERY ON FEATURE SERVER FSPTC235 IS...->
RESULT ->
QVT query has timed out
QUERYSTATUS -> Miscellaneous Failure
Reply : Success:
CLI>
```

There is no response from the SCP. Contact the SCP provider to find out why there is no error response returned from the SCP.

## Missing Mandatory Parameter

The user performs a query but does not provide all required parameters. The error response is similar to the following example:

```
CLI> query toll-free; called-dn=8002550002; user-type=calling-dn; user-id=2182640018;
lata=100; bearer-capability=speech; trigger-criteria=9;
Required attributes missing:
opc_id
CLI>
```

Supply all required parameters for the query. To view a list of parameters required for a command, enter a question mark (?) after the partial command. For example, query lldb? will display a list of required parameters for a LIDB query.

## Advanced Intelligent Network 0.1 Query Attempted for IN/1 Configuration

An AIN0.1 Toll-Free query has been performed, but the system specifies that the Toll-Free subsystem is IN/1. The error response is similar to the following example:

```
CLI> query toll-free; called-dn=8002550002; user-type=calling-dn; user-id=2182640018;
lata=100; bearer-capability=speech; trigger-criteria=9, opc-id=opc;
Reply : Failure: Missing CALLING_DN for the IN/1 query
CLI>
```

Reissue the command in the IN/1 format. To see what message type is specified for the Toll-Free subsystem, enter the following command:

```
CLI> query toll-free-msg-type; opc-id=opc;
MESSAGE-TYPE=IN1
Reply : Success:
```

## IN/1 Query Attempted for Advanced Intelligent Network 0.1 Configuration

An IN/1 Toll-Free query has been performed, but the system specifies that the Toll-Free subsystem is AIN 0.1. The error response is similar to the following example:

```
CLI> query toll-free; called-dn=8002550002; calling-dn=2182640018; lata=100;
trigger-criteria=9; opc-id=opc;
Reply : Failure: Missing USER_TYPE for the AIN 0.1 query
CLI>
```

Reissue the command in the AIN 0.1 format. To see what message type is specified for the Toll-Free subsystem, enter the following command:

```
CLI> query toll-free-msg-type; opc-id=opc;
MESSAGE-TYPE=AIN01
Reply : Success:
CLI>
```

## Parameter Boundary Error

The query can fail if you enter invalid data for a specific parameter. In the following example, a value outside the boundary of expected values for the trigger-criteria parameter has been specified.

```
CLI> query toll-free; called-dn=8002550002; calling-dn=2182640018; lata=100;
trigger-criteria=12; opc-id=opc;
Invalid parameter value.
trigger_criteria=12; Enter one of the following values: [3,6,7,8,9,10].
CLI>
```

To resolve this error, enter a valid value for the specified parameter.

## Record Does Not Exist

In the following example, a value has been entered for a lata that has not been provisioned:

```
CLI> query toll-free; called-dn=8002550002; calling-dn=2182640018; lata=101;
trigger-criteria=9; opc-id=opc;
Reply : Failure: LATA 101 does not exist
CLI>
```

To resolve this error, enter a provisioned local access and transport area (LATA).

## Local Network Failure

When communication is lost between the Cisco BTS 10200 Softswitch and the IP transfer point (ITP) gateway, a local network failure may occur. The most likely reason for this error is that the SCTP association is Out Of Service. The error response is similar to the following example:

```
CLI> query toll-free; called-dn=8002550002; calling-dn=2182640018; lata=100;
trigger-criteria=9; opc-id=opc;
QUERY ON FEATURE SERVER FSAIN205 IS...->
RESULT->
MTP failure - occurs at SP (PC7-44-1, SSN=254)
QUERYSTATUS -> Network Failure
Reply : Success:
CLI>
```

Perform the following to diagnose the problem:

- Execute the query again with the table-info option set to yes
- Determine the status of the SCTP associations used for this command. If the associations are Out Of Service, control the associations back into service.

## Remote Network Failure

A failure has occurred at a point code other than the OPC. The query response will specify what problem has occurred and at which point code the problem is detected. In the following example, the point code of the signal transfer point (STP) is reporting a failure because there is no Global Title Translation entry in the STP global text telephony (GTT) database for the calling-dn.

```
CLI> query lldb; calling-dn=9823456789; opc-id=opc;
QUERY ON FEATURE SERVER FSPTC235 IS...->
RESULT ->
No translation for this specific address - occurs at SP (PC=1-101-0, SSN=0)
QUERYSTATUS -> Network Failure
Reply : Success:
CLI> status sctp-assoc;
```

To resolve this error, add an entry to the STP GTT database to translate the calling-dn and route the query request to the LIDB subsystem on the SCP.

## Query Verification Tool Measurements

Table 15-2 identifies the measurements generated by the AIN Feature Server for the QVT feature.

**Table 15-2 QVT AIN Tools Counters**

| Counter Label              | Counter Description                                                                                                                                     |
|----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------|
| TOOLS_LNP_QUERY_ATTMP      | The total number of times the reporting feature server received a request to perform an LNP query from the QVT tool.                                    |
| TOOLS_LNP_QUERY_SUCC       | The total number of times the reporting feature server received a request to perform an LNP query from the QVT tool and completed it successfully.      |
| TOOLS_TOLLFREE_QUERY_ATTMP | The total number of times the reporting feature server received a request to perform a Toll Free query from the QVT tool.                               |
| TOOLS_TOLLFREE_QUERY_SUCC  | The total number of times the reporting feature server received a request to perform a Toll Free query from the QVT tool and completed it successfully. |

Table 15-3 identifies the measurements generated by the POTS Feature Server for the QVT feature.

**Table 15-3 QVT POTS Tools Counters**

| Counter Label          | Counter Description                                                                                                                                 |
|------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------|
| TOOLS_LIDB_QUERY_ATTMP | The total number of times the reporting feature server received a request to perform an LIDB query from the QVT tool.                               |
| TOOLS_LIDB_QUERY_SUCC  | The total number of times the reporting feature server received a request to perform an LIDB query from the QVT tool and completed it successfully. |

## Translation Verification Tool

This section describes the TVT and includes the following sections:

- [Overview, page 15-26](#)
- [Command Format, page 15-26](#)
- [Response Format, page 15-27](#)
- [Translation Verification Tool Measurements, page 15-28](#)

### Overview

The TVT is a diagnostic tool that simulates a call from the originator to a specific destination based on dialed digits. It enables a user to check system translations and determine if routing will occur as expected without making a call.

### Command Format

The TVT command uses the following format:

```
translate <line|trunk>; parameter=value;
```



**Examples** translate line calling-dn=2189722345; called-dn=8002550005

|                           |              |                                                                                 |
|---------------------------|--------------|---------------------------------------------------------------------------------|
| <b>Syntax Description</b> | * Calling-DN | The caller's directory number. VARCHAR(10): 10 digits in the format npaxxxxxxx. |
|                           | Called-DN    |                                                                                 |

**Examples** translate trunk tgn-id= 1; called-dn=7034321234;

|                           |             |
|---------------------------|-------------|
| <b>Syntax Description</b> | * Called-DN |
|                           | * Tgn-ID    |
|                           | GAP         |

## Response Format

Translation is the process of determining the destination of a call based on the dialed digits. The TVT performs translations and returns the tables traversed in order to reach the destination number. It does not complete a call but only allows you to view the route of the call.

The following example illustrates an incoming line call terminating to a trunk.

```
CLI> translate line calling-dn=9722331286;called-dn=7034321234;
```

TABLE: SUBSCRIBER

```
ID=sub1_ata2;CATEGORY=INDIVIDUAL;NAME=sub1;STATUS=ACTIVE;DN1=9722331003;PRIVACY=NONE;RING_
TYPE_DN1=1;TERM_ID=a00/1;MGW_ID=ata2;PIC1=NONE;PIC2=NONE;PIC3=NONE;GRP=N;USAGE_SENS=Y;SUB_
PROFILE_ID=northtexas;TERM_TYPE=TERM;IMMEDIATE_RELEASE=N;TERMINATING_IMMEDIATE_REL=N;SEND_
BILLING_DN=N;SEND_BDN_AS_CPN=N;SEND_BDN_FOR_EMG=N;
```

TABLE: SUBSCRIBER\_PROFILE

```
ID=northtexas;DIAL_PLAN_ID=dp1;LOCAL_PFX1_OPT=NR;TOLL_PFX1_OPT=RQ;POP_ID=1;OLI=0;EA_USE_PI
C1=Y;
```

TABLE: DIAL\_PLAN\_PROFILE

```
ID=dp1;DESCRIPTION=dialingplanprofile;NANP_DIAL_PLAN=Y;DNIS_DIGMAN_ID=dp1;
```

TABLE: DIAL\_PLAN

```
ID=dp1;DIGIT_STRING=408555;DEST_ID=sspldest;SPLIT_NPA=NONE;DEL_DIGITS=0;MIN_DIGITS=10;MAX_
DIGITS=10;NOA=NATIONAL;
```

TABLE: DESTINATION

```
DEST_ID=sspldest;CALL_TYPE=LOCAL;ROUTE_TYPE=ROUTE;ROUTE_GUIDE_ID=ssplrg;ZERO_PLUS=N;INTRA_
STATE=Y;GAP_ROUTING=N;CLDPTY_CTRL_REL_ALWD=N;TABLE: ROUTE_GUIDE
ID=ssplrg;POLICY_TYPE=ROUTE;POLICY_ID=ssplroute;
```

TABLE: ROUTE

```
ID=ssplroute;TGN1_ID=1;DEL_DIGITS1=0;DEL_DIGITS2=0;DEL_DIGITS3=0;DEL_DIGITS4=0;DEL_DIGITS5
=0;DEL_DIGITS6=0;DEL_DIGITS7=0;DEL_DIGITS8=0;DEL_DIGITS9=0;DEL_DIGITS10=0;TG_SELECTION=RR;
```

TABLE: TRUNK\_GRP

```
ID=1;CALL_AGENT_ID=CA146;TG_TYPE=SS7;NUM_OF_TRUNKS=24;DPC=1-12-1;TG_PROFILE_ID=ssp1-tg-profile;STATUS=INS;DIRECTION=BOTH;SEL_POLICY=ASC;GLARE=EVEN;ALT_ROUTE_ON_CONG=N;SIGNAL_PORTED_NUMBER=N;POP_ID=1;REMOTE_SWITCH_LRN=2122129999;DIAL_PLAN_ID=dp19;DESCRIPTION=TG to BTS12;DEL_DIGITS=0;OPER_STATUS=NF;TRAFFIC_TYPE=TANDEM;ANI_BASED_ROUTING=N;CLLI=DAL177DS3;CALL_CTRL_ROUTE_ID=bts12-ccroute1;MGCP_PKG_TYPE=T;ANI_SCREENING=N;SEND_RDN_AS_CPN=N;
```

```
Reply :Success:
```

```
CLI>
```

## Translation Verification Tool Measurements

Table 15-4 identifies the measurements generated by the TVT Tool.

**Table 15-4** TVT Tool Counters

| Counter Label              | Counter Description                                                                                                                                     |
|----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------|
| TOOLS_LNP_QUERY_ATTMP      | The total number of times the reporting feature server received a request to perform an LNP query from the QVT tool.                                    |
| TOOLS_LNP_QUERY_SUCC       | The total number of times the reporting feature server received a request to perform an LNP query from the QVT tool and completed it successfully.      |
| TOOLS_TOLLFREE_QUERY_ATTMP | The total number of times the reporting feature server received a request to perform a Toll Free query from the QVT tool.                               |
| TOOLS_TOLLFREE_QUERY_SUCC  | The total number of times the reporting feature server received a request to perform a Toll Free query from the QVT tool and completed it successfully. |

## Using Query Verification Tool and Translation Verification Tool Together

It may be necessary to use both QVT and TVT queries to diagnose routing of a call. If the results of a translate command indicate that a toll-free or LNP query is generated, execute the QVT query. Use the results of the QVT query to generate another TVT query.

The following example illustrates verifying routing of a call from (972) 233-1286 to (800) 255-3002:

### Step 1 Execute a TVT translate command:

```
CLI> translate line calling-dn=9722331286; called-dn=8002553002;
```

```
TRANSLATE LINE ON CALL AGENT CA146 IS...->
TABLEINFO ->
*****TOLL FREE CALL NEEDS AN 800 QUERY*****
```

```
Reply : Success:
```

```
CLI>
```

- Step 2** The translate command indicates that a Toll-Free query is required. Perform the QVT query to do the number translation.

```
CLI> query toll-free called-dn=8002553002; calling-dn=9722331286; lata=100; opc-id=opc;
```

```
TOLL FREE QUERY ON FEATURE SERVER FSAIN520 IS...->
```

```
RESULT->
```

```
OPC=7-2-1
```

```
SSN=254
```

```
TT=254
```

```
SCP-Point-Code=1-101-0
```

```
Message-Type=IN/1
```

```
Called Number=8002553002
```

```
Translated Number=7034323002
```

```
Carrier=0000
```

```
Reply : Success:
```

```
CLI>
```

- Step 3** The translated number returned by the QVT query can now be used in a TVT translate command to verify call routing.

```
CLI> translate line calling-dn=9722331286;called-dn=7034323002;
```

```
TRANSLATE LINE ON CALL AGENT CA146 IS... ->
```

```
TABLEINFO ->
```

```
TABLE: SUBSCRIBER
```

```
ID=sub_1_6;CATEGORY=INDIVIDUAL;NAME=sub16;STATUS=ACTIVE;ADDRESS1=1651 n glenville suite
200;ADDRESS2=Richardson tx
75081;BILLING_DN=9722331286;DN1=9722331286;PRIVACY=NONE;RING_TYPE_DN1=1;TERM_ID=aaln/S1/6;
MGW_ID=c2421_1;PIC1=NONE;PIC2=NONE;PIC3=NONE;GRP=N;USAGE_SENS=Y;SUB_PROFILE_ID=sub_pmlhg_p
rof1;TERM_TYPE=TERM;IMMEDIATE_RELEASE=N;TERMINATING_IMMEDIATE_REL=N;SEND_BILLING_DN=N;SEND
_BDN_AS_CPN=N;SEND_BDN_FOR_EMG=N;
```

```
TABLE: SUBSCRIBER_PROFILE
```

```
ID=sub_pmlhg_prof1;DIAL_PLAN_ID=dp1;LOCAL_PFX1_OPT=NR;TOLL_PFX1_OPT=RQ;LSA=9;POP_ID=1;OLI=
0;EA_USE_PIC1=N;
```

```
TABLE: DIAL_PLAN_PROFILE
```

```
ID=dp1;DESCRIPTION=dialing plan profile ID 1;NANP_DIAL_PLAN=Y;DNIS_DIGMAN_ID=dp_svc;
```

```
TABLE: DIAL_PLAN
```

```
ID=dp1;DIGIT_STRING=703432;DEST_ID=ssp1-dest;SPLIT_NPA=NONE;DEL_DIGITS=0;MIN_DIGITS=7;MAX_
DIGITS=10;NOA=NATIONAL;
```

```
TABLE: DESTINATION
```

```
DEST_ID=ssp1-dest;CALL_TYPE=LOCAL;ROUTE_TYPE=ROUTE;ROUTE_GUIDE_ID=ssp1-rg;ZERO_PLUS=N;INTR
A_STATE=Y;GAP_ROUTING=N;CLDPTY_CTRL_REL_ALWD=N;
```

```
TABLE: ROUTE_GUIDE
```

```
ID=ssp1-rg;POLICY_TYPE=ROUTE;POLICY_ID=ssp1-route;
```

```
TABLE: ROUTE
```

```
ID=ssp1-route;TGN1_ID=3;DEL_DIGITS1=0;DEL_DIGITS2=0;DEL_DIGITS3=0;DEL_DIGITS4=0;DEL_DIGITS5=0;DEL_DIGITS6=0;DEL_DIGITS7=0;DEL_DIGITS8=0;DEL_DIGITS9=0;DEL_DIGITS10=0;TG_SELECTION=RR;
```

```
TABLE: TRUNK_GRP
```

```
ID=3;CALL_AGENT_ID=CA146;TG_TYPE=SS7;NUM_OF_TRUNKS=24;DPC=1-12-1;TG_PROFILE_ID=ssp1-tg-profile;STATUS=INS;DIRECTION=BOTH;SEL_POLICY=ASC;GLARE=EVEN;ALT_ROUTE_ON_CONG=N;SIGNAL_PORTED_NUMBER=N;POP_ID=1;REMOTE_SWITCH_LRN=2122129999;DIAL_PLAN_ID=dp19;DESCRIPTION=TG to BTS12;DEL_DIGITS=0;OPER_STATUS=NF;TRAFFIC_TYPE=TANDEM;ANI_BASED_ROUTING=N;CLLI=DAL177DS3;CALL_CTRL_ROUTE_ID=bts12-ccroute1;MGCP_PKG_TYPE=T;ANI_SCREENING=N;SEND_RDN_AS_CPN=N;
```

```
Reply : Success:
```

```
CLI>
```

## Network Loopback Test for Network-based Call Signaling/Media Gateway Control Protocol Endpoints

This section describes the feature that provides the capability to perform network loopback test on any line side PacketCable Network-based Call Signaling protocol specification/Media Gateway Control Protocol (NCS/MGCP) Residential Gateways initiated from designated test endpoints. This document also describes enhancements to the TDM bearer path test call feature.

This section contains the following:

- [Overview](#)
- [Restrictions](#)
- [Installing](#)
- [Configuring](#)
- [Using/Operating the Network Loopback Test for Network-based Call Signaling/Media Gateway Control Protocol Endpoints](#)

### Overview

The Network Loopback Test for NCS/MGCP Endpoints feature provides a testing device with the capability to perform network loopback tests from any line side NCS/MGCP residential gateways or media termination adapters (MTAs). These loopback tests are initiated from designated test endpoints (subscribers) controlled by the Cisco BTS 10200 Softswitch.

## Restrictions

Although you can test this feature by using the regular MTA as the testing device by configuring the endpoints as subscriber terminations in Cisco BTS 10200 Softswitch, you need special test equipment such as BRIX if voice quality testing needs to be done.

You should configure the testing and tested devices on the same Call Agent. The Cisco BTS 10200 Softswitch cannot perform network loopback test calls that originate from another switch and does not route calls from a testing device on an H.323 or SIP interface.

**Note**

You cannot perform the network loopback test if the status of the subscriber to be tested is **unequipped (UEQP)** or **operational-out-of-service (OOS)**.

## Installing

The following items must be configured:

- Test origination endpoints as trunks instead of line.
- Special dial plan and destination with CALL-TYPE TEST-CALL; CALL-SUBTYPE=NLB-TEST).

## Configuring

To configure the originating line (media gateway profile) for the testing device, use the following procedure:

- 
- |               |                                                                                                                                        |
|---------------|----------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | Configure the media gateway for the testing device as RGW (residential gateway):<br><br><b>MGW-PROFILE::TYPE=RGW</b>                   |
| <b>Step 2</b> | Associate the media gateway to the MGW-PROFILE specific to network loopback test origination:<br><br><b>MGW-PROFILE::SPARE2-SUPP=Y</b> |
| <b>Step 3</b> | Configure all test lines in the testing device as subscriber terminations.                                                             |
-

## Configuration Examples

The following example describes the steps required to configure the originating line (media gateway profile) to identify a network loopback call.



### Note

These tasks include examples of CLI commands that illustrate how to provision the specific feature. Most of these tables have additional tokens that are not included in the examples. For a complete list of all CLI tables and tokens, see the *Cisco BTS 10200 Softswitch Command Line Interface Reference Guide*.

|        | Command or Action                                                                                                                                                                                                                                                                                                                                                 | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|--------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | Configure the basic office database (such as Call-Agent; POP; Office).                                                                                                                                                                                                                                                                                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Step 2 | Enter the following CLI commands:<br><br><pre>add mgw-profile id=mta1; SPARE2-SUPP=Y; add mgw id=brix; mgw-profile=mta1; tasp-addr=mta.abc.com; call-agent-id=CA146</pre>                                                                                                                                                                                         | Configures the MGW as a testing device.<br><br><b>Note</b> “brix” is an example of a test equipment that can be used.                                                                                                                                                                                                                                                                                                                                                               |
| Step 3 | Enter the following CLI commands:<br><br><pre>add termination prefix=aaln/s1/; port-start=1; port-end=2; type=LINE; mgw-id= brix; add subscriber-profile id=dp5; dial-plan-id=dp1; pop-id=1; add sub id=Abc; category=INDIVIDUAL; name=ABC; status=ACTIVE; billing-dn= 555-123-4567; ring-type-dn1= 1; term-id=aaln/S1/1; sub-profile-id=dp5; mgw-id=c2421;</pre> | Configures the test originating subscriber lines on the testing device.<br><br>Where: <ul style="list-style-type: none"> <li><b>brix</b> is an example of a test equipment</li> <li><b>555-123-4567</b> is an example of a subscriber number</li> </ul> <b>Note</b> If you want calls to terminate on the subscriber testing device, you must assign <b>dn1</b> when the subscriber is provisioned, as shown in the following example:<br><br><b>dn1= &lt;subscriber number&gt;</b> |

## Using/Operating the Network Loopback Test for Network-based Call Signaling/Media Gateway Control Protocol Endpoints

This section explains how to perform the following task:

- [Dedicated Test Trunk Group](#)
- [Shared Test Trunk Group](#)
- [Configuring the Originating Trunk Group](#)

To use this feature, place a call from the testing device subscriber to any MGCP subscriber to be tested. For example, if the testing device is an MGCP telephone, dial the number of the subscriber to be tested.

## Dedicated Test Trunk Group

The Cisco BTS10200 Softswitch allows NCS/MGCP endpoints in a trunk group to be provisioned as a test trunk group with certain test attributes.

The test attributes consist of whether the incoming calls arriving on these test trunk groups will trigger the Cisco BTS10200 Softswitch to perform call completion via Network Loopback (NLB) or Network Continuity Test (NCT) method toward the eMTA. Hence, the category of the test is pre-provisioned on these incoming test dedicated trunk groups—all calls from a particular test trunk group invoke the same test category toward the eMTAs while calls from another test trunk group perform a different test category. The call from the testing device addresses the eMTA directory number (DN) as any regular digit that can be dialed.

The called party number format is:

<Test-data>

Where:

<Test-data> = DN (for example, the NCS/MGCP dialed digits signaled to the Cisco BTS10200 Softswitch are in the form of a 10-digit DN such as 2145261234, or <TG>TM> (Trunk group and trunk member)

The steps for configuring the originating trunk group are:

- 
- |               |                                                                                                                                                                                                       |
|---------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | Add a trunk group for the testing device as CAS trunk group (TRUNK-GRP::TG-TYPE=CAS).                                                                                                                 |
| <b>Step 2</b> | Associate the trunk group to CAS-TG-PROFILE specific to network loopback test origination type (CAS-TG-PROFILE::TEST-LINE=Y;<br>CAS-TG-PROFILE::TEST-LINE-TYPE=NLB-LINE/NCT-LINE/NLB-TRUNK/NCT-TRUNK. |
| <b>Step 3</b> | Add all test lines in the testing device as trunk termination.                                                                                                                                        |
- 

## Shared Test Trunk Group

In addition to dedicated test trunk groups, the Cisco BTS 10200 Softswitch allows a shared test trunk group, where the category of the test to be run is specified by the test-prefix. Cisco BTS 10200 Softswitch allows a test trunk group to be associated with a test dial plan. The test trunk group can be either the IP or CAS TDM trunks. Incoming calls from the network on these trunk groups will be analyzed according to a pre configured test dial plan. The following is the format of dialed digits for these incoming test calls.

Called party number format:

<Test-prefix><Test-data>

Where:

- **<Test-prefix>** is a string of digits that denote the test category. Operator must configure the definition (recommended as a pattern of 1 to 6 digits, the BTS10200 Softswitch will perform the longest match) of the test prefix and its length, whether it is an IP or TDM testing. If it is TDM testing, the traditional 1xx test type value is expected or the general TDM test category needs to be specified (for example, 199) when the route out DN testing is going to be used.

For example, test-prefix 152 may denote NLB IP testing, or 105 may convey the TDM 105 test-type, or 199 may be defined to specify the TDM route out DN testing, or 153 is the configured prefix for NCT.

- **<Test-data>** is a string that depends on the test-prefix content.

## Configuring the Originating Trunk Group

The following are the steps for configuring the originating trunk group:

- 
- Step 1** Add a trunk-group for the testing device as CAS trunk-group (TRUNK-GRP::TG-TYPE=CAS).
  - Step 2** Associate the trunk-grp to CAS-TG-PROFILE specific to network loopback test origination (CAS-TG-PROFILE::TEST-LINE=Y; CAS-TG-PROFILE::TEST-LINE-TYPE=NTE).
  - Step 3** Configure all test lines in Testing device as trunk-termination.
  - Step 4** Configure the test dial plan destination with the exact type of test call.
  - Step 5** Configure the main subscriber ID for testing trunk-grp.
  - Step 6** Configure the digit map for collecting prefixed digits and associate it to the SUBSCRIBER-PROFILE table.



# Session Initiation Protocol Subscriber Registration Status Check

The SIP subscriber registration status check CLI command (sip-reg-contact) is used to check the registration status of a SIP subscriber. The need to check the registration status of a SIP subscriber may arise, for example, when a subscriber complains about not being able to receive calls. The first item to check would be the registration status using the sip-reg-contact CLI command. The next item would be to check for events regarding authentication failures and etc.

The following examples show the usage of the sip-reg-contact CLI command. The first example provides an example of an expired contact and the second example provides an example of a registered contact or current contact.

## Example 1:

CLI to check the registration status of an address of record (AOR).

```
CLI>status sip-reg-contact;
CLI>AOR_ID=4692551119@sia-SYS44CA146.ipclab.cisco.com;
AOR ID -> 4692551119@sia-SYS44CA146.ipclab.cisco.com
USER -> 4692551119
HOST -> 10.89.220.21
PORT -> 5060
USER TYPE -> USER_PHONE_TYPE
EXPIRES -> 3600
EXPIRETIME -> Tue Oct 7 12:13:11 2003
STATUS -> EXPIRED CONTACT
Reply : Success:
```

## Example 2:

CLI to check the registration status of an AOR.

```
CLI>status sip-reg-contact;
CLI>AOR_ID=4692551001@sia-SYS44CA146.ipclab.cisco.com;
AOR ID -> 4692551001@sia-SYS44CA146.ipclab.cisco.com
USER -> 4692551001
HOST -> 10.89.223.193
PORT -> 5060
USER TYPE -> USER_IP_TYPE
EXPIRES -> 3600
EXPIRETIME -> Thu Oct 23 16:23:48 2003
STATUS -> REGISTERED CONTACT
Reply : Success:
```

# System Health Report

The System Health Report (system-health) (SHR) allows the retrieval of the status of various processes within the Cisco BTS 10200 Softswitch.

Use the following command example to run a SHR immediately:

```
CLI>report system-health period=720;
```

**PERIOD** The amount of time to collect back to in hours. INTEGER: 1–720 (Default = 24).

The SHR command can be used in conjunction with the command scheduler. Using the command scheduler, the SHR runs at periodic intervals collecting the last 24 hours (configurable) worth of data. Upon initial installation and startup, there is an SHR command already scheduled to execute at midnight every 24 hours.

To schedule multiple SHR command(s) at different times, the command scheduler add command can be issued multiple times:

```
CLI>add scheduled-command verb=report; noun=system-health; <recurrence=DAILY>;
<start-time=...>; <keys=period>; <values=...>
```

Use the following command to remove any scheduled SHR command(s):

```
CLI>delete scheduled-command id=NNN
```

Use the following command to obtain an ID number and view the list of scheduled command(s):

```
CLI>show scheduled-command verb=report; noun=system-health
```

To reschedule an SHR command for another time, change the recurrence, or change the collection period, use the following command:

```
CLI>change scheduled-command id=NNN; <recurrence=DAILY>; <start-time=...>; <keys=period>;
<values=...>
```



## CHAPTER 16

# Disaster Recovery Procedures

---

**Revised: October 23, 2008, OL-11335-06**

Please refer to the *Cisco BTS 10200 Softswitch Operations and Maintenance Guide for Releases 4.1, 4.2, and 4.4, Chapter 21* for the disaster recovery procedures.





## CHAPTER 17

# Disk Replacement

---

**Revised: October 23, 2008, OL-11335-06**

Refer to the *Cisco BTS 10200 Softswitch Operations and Maintenance Guide for Releases 4.1, 4.2, and 4.4, Chapter 23* for the disk replacement procedures.





## APPENDIX **A**

# System Usage of MGW Keepalive Parameters, Release 4.4.x

---

**Revised: October 23, 2008, OL-11335-06**

This appendix explains how the Cisco BTS 10200 Softswitch determines the connectivity status between itself and a media gateway (MGW). The Cisco BTS 10200 Softswitch executes a keepalive (KA) process that includes the transmission of audit-endpoint (AUEP) messages to MGCP, TGCP, and NCS based MGWs.

This appendix also describes a special set of provisionable parameters that you can adjust if there are network bandwidth or reliability issues, or if a MGW is slow in responding to commands from the Call Agent.

# Provisionable Parameters

The following tokens are involved in KA process:

- In the [mgw-profile](#) table:
  - keepalive-method (default = AUEP)
  - mgcp-keepalive-retries (default = 3)
  - mgcp-max1-retries (default = 2)
  - mgcp-max2-retries (default = 3)
  - mgcp-keepalive-interval (default = 60 seconds)
  - mgcp-t-tran (default = 400 milliseconds)
- In the [call-agent](#) table:
  - mgw-monitoring-enabled (default=Y)

The system behavior described in this document assumes that all of the tokens in the above list are set to their default values. This has the following effect:

- Enabling the KA process—Using the default values of **mgw-monitoring-enabled** (Y) and **keepalive-method** (AUEP) enables the sending of AUEP messages from the Cisco BTS 10200 Softswitch to the MGW.



## Note

We recommend that you keep these tokens set to their default values (which enables the KA process) unless you have some other method of determining MGW connectivity status.

- Tuning the KA process—The other mgw-profile tokens in the above list have numerical values, and the default values typically work well for most systems. The interaction among these tokens is described in this document. We do not recommend that you modify these values unless you experience problems with bandwidth, reliability, or response times in your network.



## Caution

Before modifying any of these numerical values (using values different than the factory default settings), thoroughly read and understand the contents of this document. If you have questions, contact your Cisco account team or Cisco TAC.



# Definitions and Additional Parameters

This section defines some of the terms used to describe the KA process.

- **KA procedure**—A series of transmissions and retransmissions of AUEP messages used to determine the MGCP connectivity status between the Cisco BTS 10200 Softswitch and the MGW. If there is a loss of connectivity, the Cisco BTS 10200 Softswitch retries the series of AUEP transmissions up to a specified number of retries before declaring the MGW to be in **down status**.
- **KA attempt**—The transmission of an AUEP message, with a defined number of retransmissions of the same AUEP message, until an ACK message is received or the defined number of retransmissions has been reached. This can include retransmissions to additional IP addresses if provisioned to do so. A KA attempt is defined as successful if an ACK is received from the MGW, and failed if no ACK is received after the defined number of AUEP retransmissions. A KA attempt is also called an AUEP transaction.
- **KA retries**—Subsequent KA attempts, sent only if the initial KA attempt fails.
- **MGW in working status**—A KA attempt to this MGW is successful (an ACK is received).
- **MGW in down status**—After a defined number of KA retry failures, the Cisco BTS 10200 Softswitch declares this MGW to be in **down status**, and continues to perform the KA procedure.

**Note**

To learn more about the MGW operational states reported by the Cisco BTS 10200 Softswitch, see the [MGW Status Command](#) in the *Cisco BTS 10200 Softswitch Operations and Maintenance Guide*.

The following parameters are also related to MGW connection status, but are not discussed in detail in this appendix. For additional details, see the *Cisco BTS 10200 Softswitch Command Line Reference Guide*.

- **Long transaction**—The **mgcp-t-longtran** field in the [mgw-profile table](#) specifies the initial MGCP transaction timeout (in seconds) after receiving a provisional response (return code 100) from the MGW. The range is 1–10 (default = 5).
- **Return code action**—The endpoint action (**ep-action**) field in the Media Gateway Control Protocol Return Code Action ([mgcp-retcode-action](#)) table specifies what action to take when an MGCP message is received from an MGW.

## Examples of Successful MGCP Message Transmissions

This section illustrates several scenarios with successful MGCP message transmissions.

**Note**

This section describes how the system sends AUEP messages. This discussion can be applied to the sending of any MGCP messages (including AUEP).

## Initial AUEP Transmission Successful

Figure A-1 illustrates the basic scenario in which the initial AUEP transmission is successful, that is, the Cisco BTS 10200 Softswitch receives an acknowledgement (ACK) message before the designated time,  $t$ , has elapsed.

The period,  $t$ , is defined as a time period equal to *the greater of* the following:

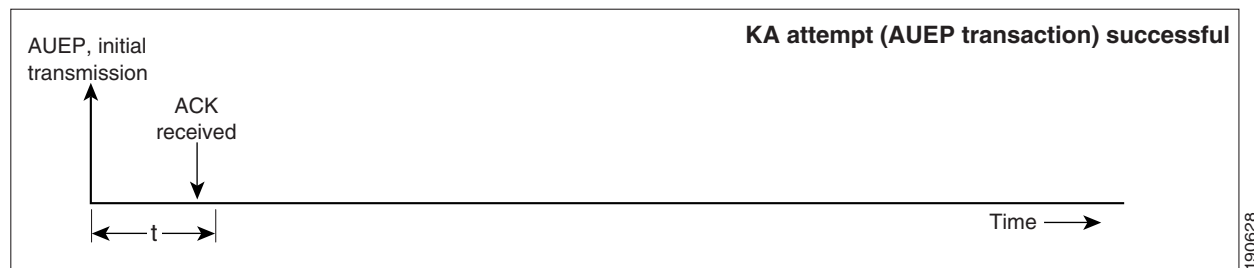
- Average response time between the sending of an MGCP message, and receiving a response.
- A specified lower limit, provisioned as **mgcp-t-tran** (default 400 milliseconds) in the **mgw-profile** table.



### Note

The drawings in this section are not to scale.

**Figure A-1** Initial AUEP Successful



## Scenarios with Retransmissions

Figure A-2 and Figure A-3 show scenarios in which a message transmission is successful (receives an ACK response) after one or more retries (retransmissions). You can adjust the parameters **mgcp-max1-retries** and **mgcp-max2-retries**, if necessary, to improve response if there are network bandwidth or reliability issues, or if a MGW is slow in responding to commands from the Call Agent. These parameters are defined as follows:

- **mgcp-max1-retries** = Number of AUEP retransmissions sent to a single IP address before selecting the next IP address for this MGW listed in the DNS server (default=2).
- **mgcp-max2-retries** = Number of AUEP retransmissions sent to the last IP address for this MGW listed in the DNS server (default=3).

The Cisco BTS 10200 Softswitch processes inbound calls for a MGW as follows, based on the values of **mgcp-max1-retries** and **mgcp-max2-retries**:

- If an inbound call for a MGW has not received an ACK and is within **mgcp-max1-retries** or **mgcp-max2-retries**, the system holds the command to the specific MGW in the command sequencer until one of the following occurs:
  - A positive response is received from the MGW. The system sends the next message that was held.
  - A negative response is received from the MGW. The system takes the recovery action specified in the **ep-action** field of the applicable Media Gateway Control Protocol Return Code Action (**mgcp-retcode-action**) table.
  - The **mgcp-max2-retries** are completed without an ACK received. Held messages are deleted.
- If an inbound call for a MGW has not received an ACK and is beyond **mgcp-max2-retries**, the system takes the following action, depending upon the specific software release:
  - In Release 4.4.0—The system declares the termination to be unreachable (TERM\_UNREACH) and expedites the MGW KA process (as described in the [“Keepalive Process” section on page A-8.](#))
  - In Release 4.4.1 and later—The system expedites the KA process (as described in the [“Keepalive Process” section on page A-8](#)) without immediately declaring the termination to be unreachable. However, if the KA process also fails, the system declares the MGW and all associated terminations to be unreachable.
  - All releases—If the system declares the termination to be unreachable, it attempts to forward the call to voice mail if provisioned. If the system attempts to terminate the call on an unreachable termination, the calling party hears an announcement; however, if an announcement is not provisioned, the caller hears a reorder tone.

Figure A-2 is applicable when a single IP address is provisioned for the MGW in the DNS server. It illustrates the scenario in which the initial AUEP transmission does not receive an ACK message, but an ACK is received in response to retries (retransmissions).

**Figure A-2** Single IP Address in DNS, ACK Received after Retries

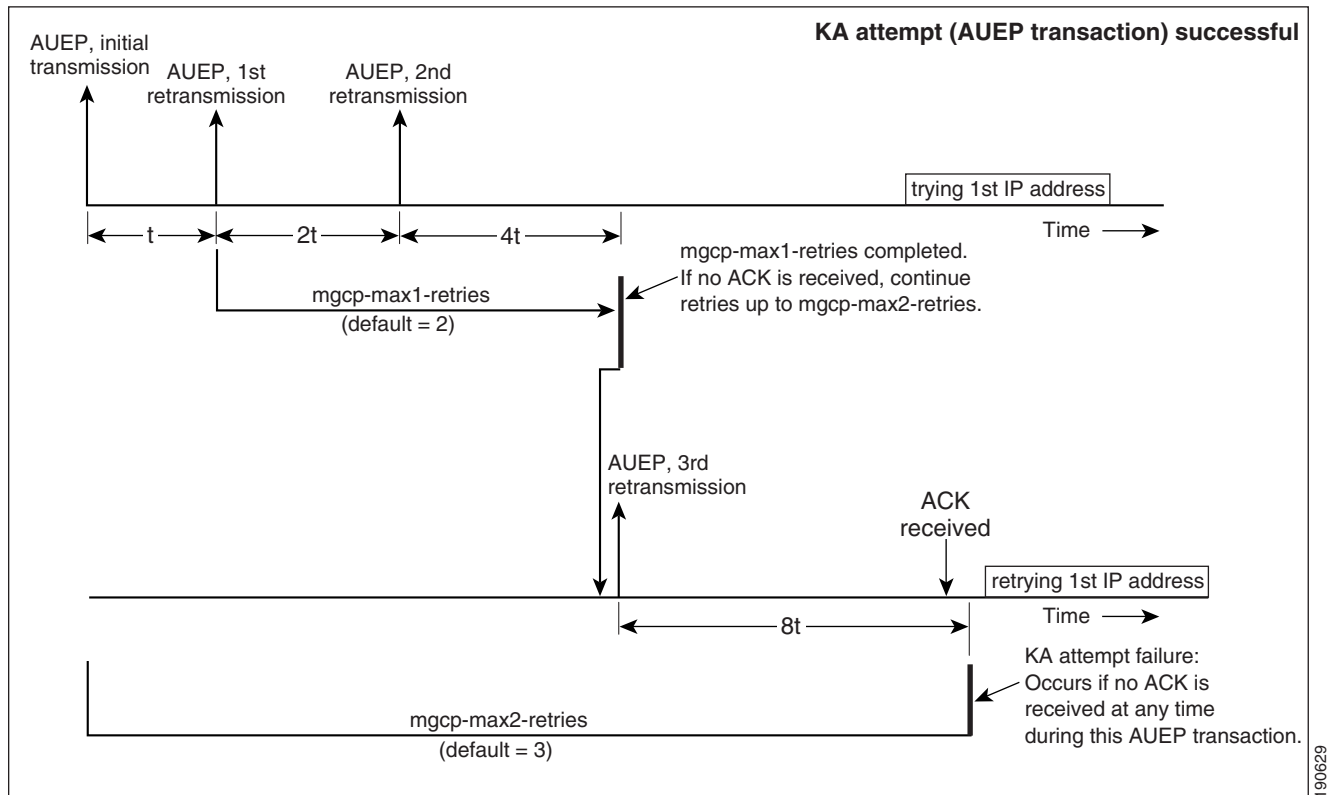
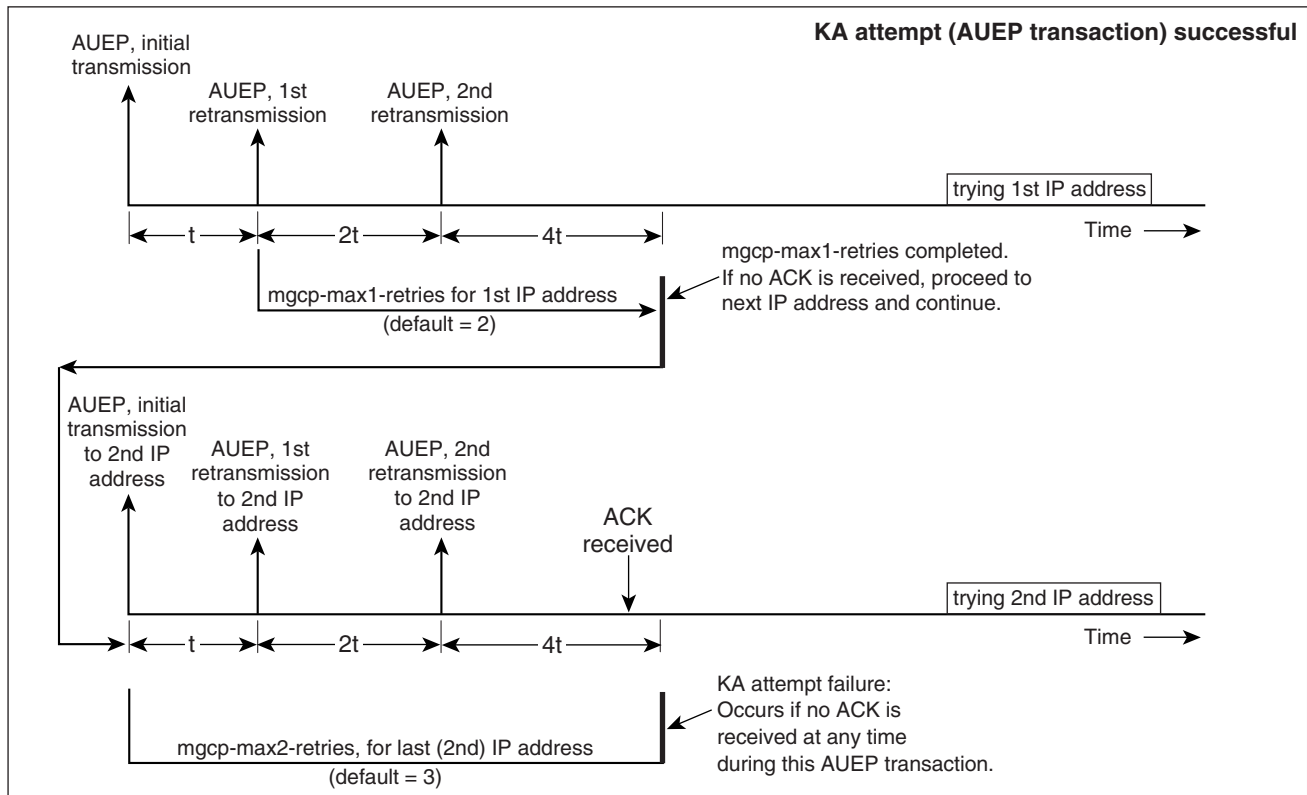


Figure A-3 is applicable when two IP addresses are provisioned for the MGW in the DNS server. It illustrates the scenario in which the initial AUEP transmission does not receive an ACK message, but an ACK is received in response to retries (retransmissions).

**Figure A-3** Two IP Addresses in DNS, ACK Received after Retries



**Note**

The system attempts up to four different IP addresses for any single MGW listed in the DNS server. (This maximum number of IP addresses is not provisionable.)

# Keepalive Process

This section describes the keepalive (KA) process. The Cisco BTS 10200 Softswitch performs KA attempts to determine whether a MGW should be considered to be in **working status** or **down status**.

There are three KA scenarios covered in this section:

- [Scenario 1—MGW Reachable](#)
- [Scenario 2 \(Special Case\)—Reachable RGW with 16 or Fewer Endpoints and No Stable Calls In Progress](#)
- [Scenario 3—MGW Unreachable](#)

**Note**

The following sections refer to two types of MGWs, residential gateways (RGWs) and trunking gateways (TGWs). A MGW is identified as either a RGW or TGW according to the provisioning of the **type** token in the **mgw** table (**type=rgw** or **type=twg**).

## Scenario 1—MGW Reachable

This scenario applies to the following types of MGWs (when the MGWs are reachable):

- Trunking gateways (TGWs), with or without stable calls in progress
- Residential gateways (RGWs) with more than 16 endpoints, with or without stable calls in progress
- RGWs with 16 or fewer endpoints and with stable call(s) in progress

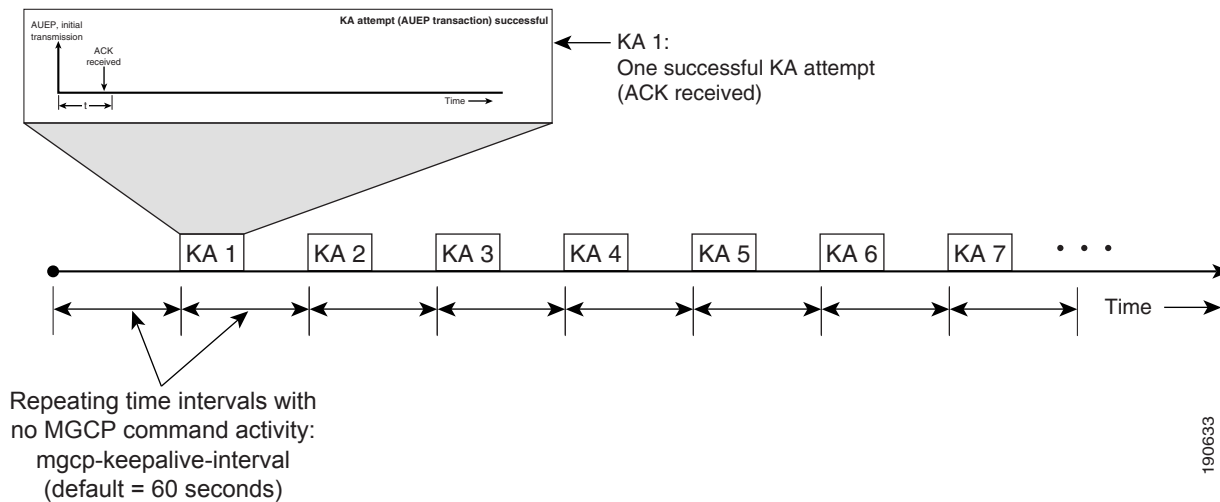
Three variations of this scenario are described in this section:

- [Basic Scenario](#)
- [MGCP Message Sent and Is Unsuccessful](#)
- [MGCP Message Sent and Is Successful](#)

## Basic Scenario

The basic scenario is shown in [Figure A-4](#). The MGW is reachable (an ACK is received during each KA attempt) and has stable calls, but no MGCP messages have been exchanged between the Cisco BTS 10200 Softswitch and the MGW for a time interval equal to the provisioned value of **mgcp-keepalive-interval** (default 60 seconds) in the **mgw-profile** table.

**Figure A-4 KA Attempts—MGW Reachable with Stable Calls**



### Note

For detailed examples of successful KA attempts, see [Figure A-1](#) through [Figure A-3](#).

The system takes the following actions in the scenario shown in [Figure A-4](#):

- If KA attempts are successful, and stable calls exist: The system continues this pattern of KA attempts ([Scenario 1—MGW Reachable](#)).
- For RGWs with 16 or fewer endpoints—If KA attempts are successful, and no stable calls exist: The system implements the KA pattern shown in Scenario 2. (See [Scenario 2 \(Special Case\)—Reachable RGW with 16 or Fewer Endpoints and No Stable Calls In Progress](#).)



### Note

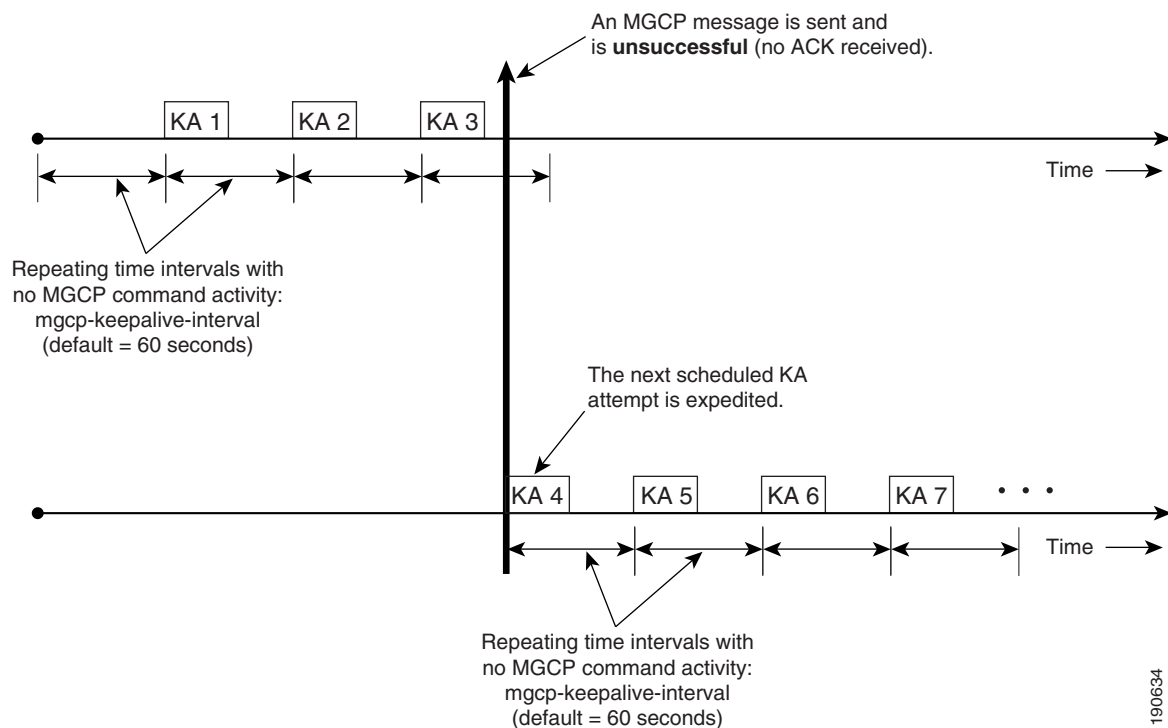
For TGWs and RGWs with more than 16 endpoints—If a KA attempt is successful, the system continues to implement Scenario 1 regardless of whether there are stable calls or not.

- If a KA attempt is unsuccessful: The system implements the KA pattern shown in Scenario 3. (See [Scenario 3—MGW Unreachable](#).)

## MGCP Message Sent and Is Unsuccessful

If the Cisco BTS 10200 Softswitch sends an MGCP message to the MGW, and the message is unsuccessful (no ACK received), the KA process is expedited even though the next KA attempt is scheduled for a later time. This condition is shown in [Figure A-5](#).

**Figure A-5** *MGW Reachable with Stable Calls, and MGCP Message Unsuccessful*

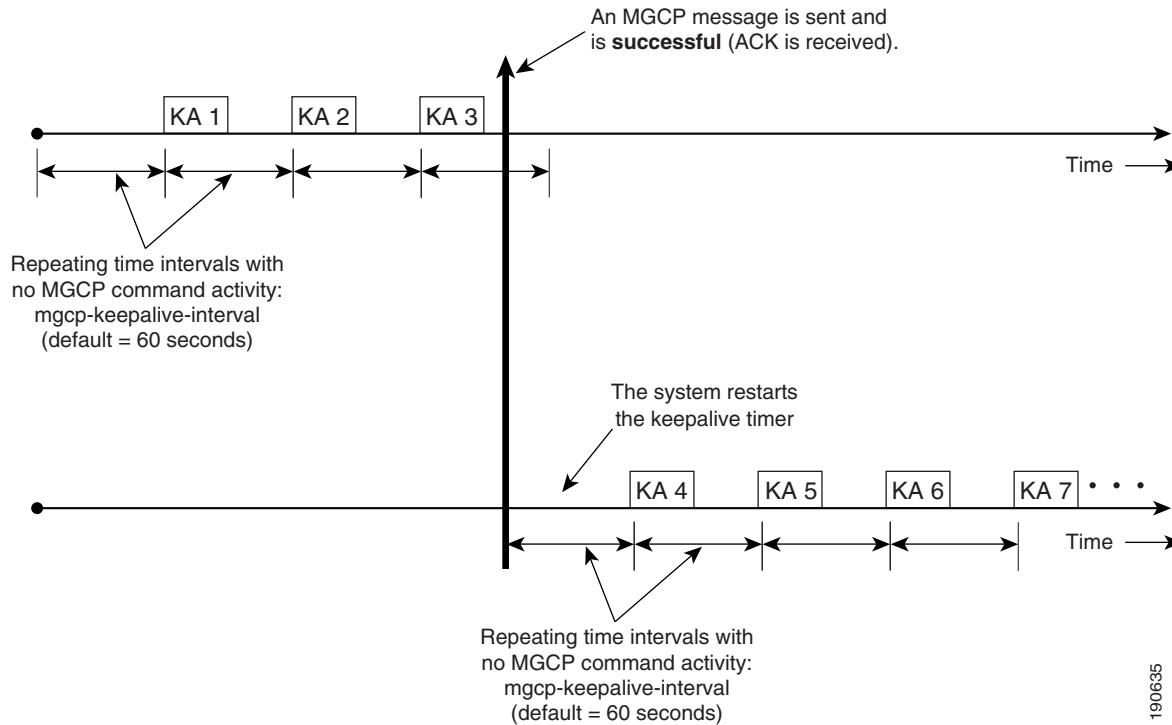




## MGCP Message Sent and Is Successful

If the Cisco BTS 10200 Softswitch sends an MGCP message to the MGW, and the message is successful (an ACK is received), the system restarts the keepalive timer. This condition is shown in [Figure A-6](#).

**Figure A-6** *MGW Reachable with Stable Calls, and MGCP Message Successful*



## Scenario 2 (Special Case)—Reachable RGW with 16 or Fewer Endpoints and No Stable Calls In Progress

This scenario is applicable to RGWs with 16 or fewer endpoints, but not to TGWs or RGWs with more than 16 endpoints. (The Cisco BTS 10200 Softswitch always uses [Scenario 1—MGW Reachable](#) procedures for reachable TGWs and reachable RGWs with more than 16 endpoints, regardless of whether there are stable calls or not.)

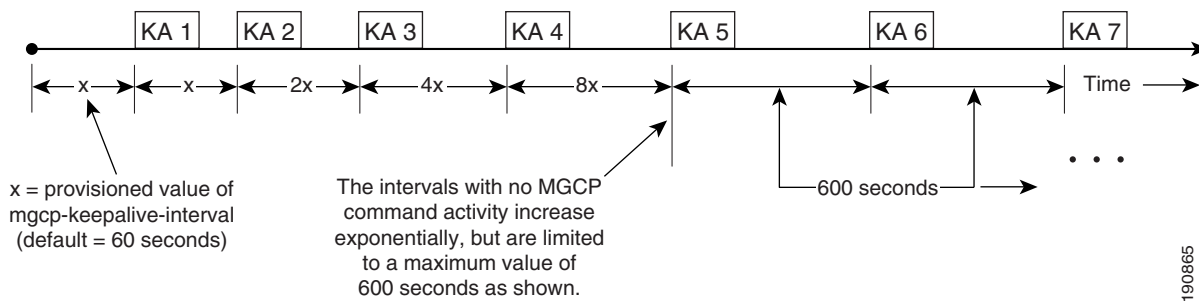
Three variations of this scenario are described in this section:

- [Basic Scenario](#)
- [MGCP Message Sent and Is Unsuccessful](#)
- [MGCP Message Sent and Is Successful](#)

## Basic Scenario

The basic scenario is shown in [Figure A-7](#). The MGW is reachable (an ACK is received during each KA attempt) and has no stable calls, and no MGCP messages have been exchanged between the Cisco BTS 10200 Softswitch and the MGW for a time interval equal to the provisioned value of **mgcp-keepalive-interval** (default 60 seconds) in the **mgw-profile** table.

**Figure A-7 KA Attempts—MGW Reachable with No Stable Calls**



### Note

For detailed examples of successful KA attempts, see [Figure A-1](#) through [Figure A-3](#).

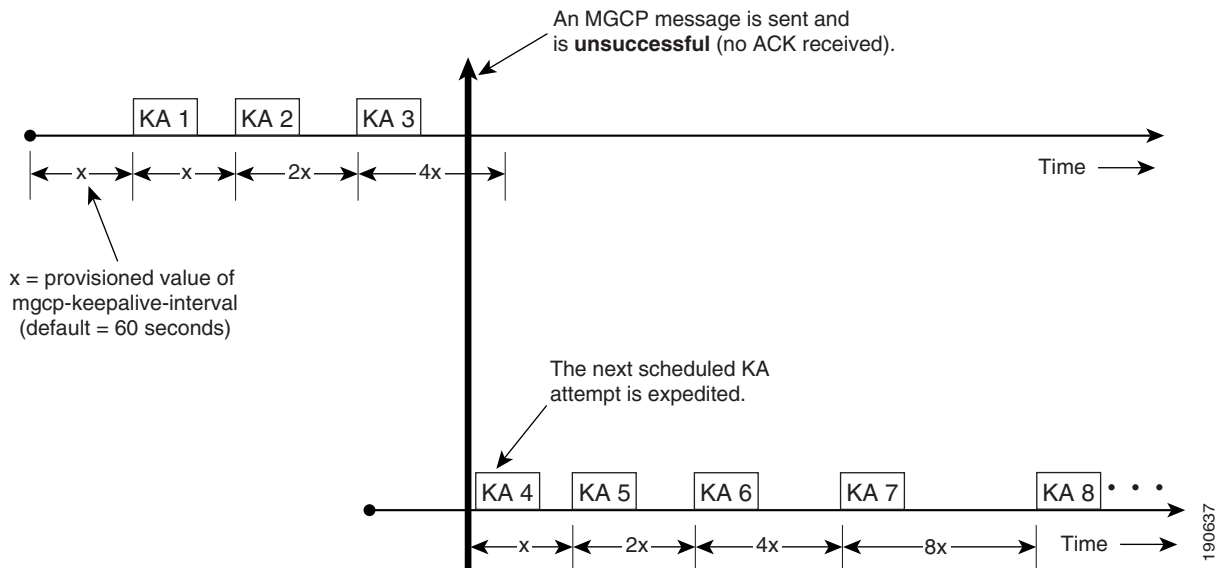
The system takes the following actions in the scenario shown in [Figure A-7](#):

- If KA attempts are successful, and stable calls exist: The system implements the KA pattern shown in Scenario 1. (See [Scenario 1—MGW Reachable](#).)
- If KA attempts are successful, and no stable calls exist: The system continues this pattern of KA attempts ([Scenario 2 \(Special Case\)—Reachable RGW with 16 or Fewer Endpoints and No Stable Calls In Progress](#)).
- If a KA attempt is unsuccessful: The system implements the KA pattern shown in Scenario 3. (See [Scenario 3—MGW Unreachable](#).)

## MGCP Message Sent and Is Unsuccessful

If the Cisco BTS 10200 Softswitch sends an MGCP message to the MGW, and the message is unsuccessful (no ACK received), the KA process is expedited even though the next KA attempt is scheduled for a later time. This condition is shown in [Figure A-8](#).

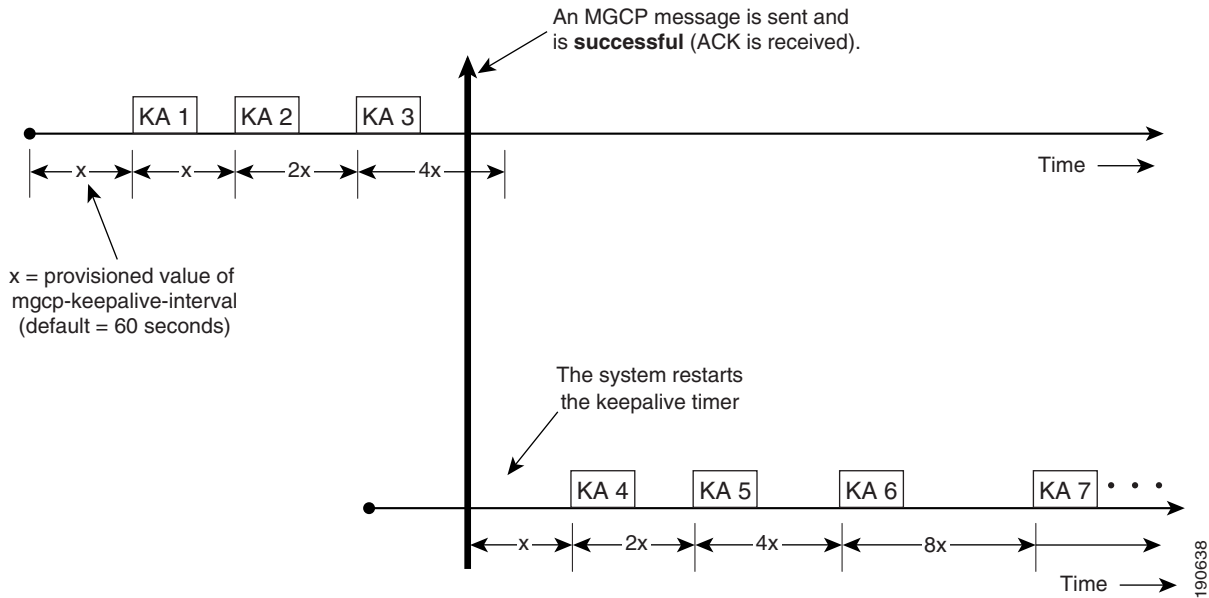
**Figure A-8** *MGW Reachable with No Stable Calls, and MGCP Message Unsuccessful*



## MGCP Message Sent and Is Successful

If the Cisco BTS 10200 Softswitch sends an MGCP message to the MGW, and the message is successful (an ACK is received), the system restarts the keepalive timer. This condition is shown in [Figure A-9](#).

**Figure A-9** *MGW Reachable with No Stable Calls, and MGCP Message Successful*



## Scenario 3—MGW Unreachable

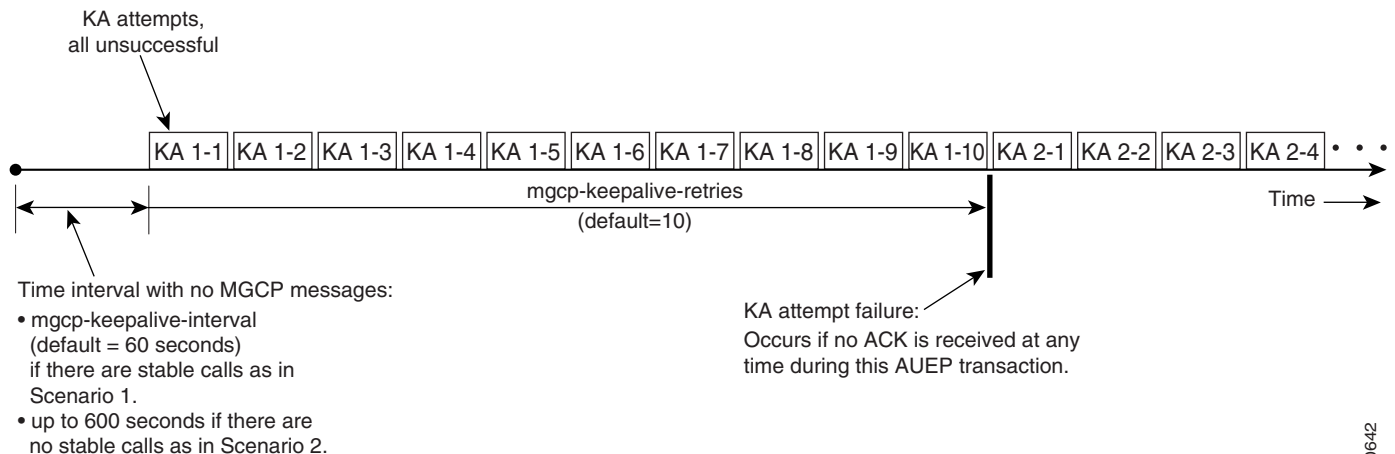
This scenario applies to residential gateways (RGWs) and trunking gateways (TGWs). Separate descriptions are provided for the following software releases:

- [Release 4.4.0—KA Attempts Unsuccessful, MGW Unreachable](#)
- [Releases 4.4.1 and Later—KA Attempts Unsuccessful, MGW Unreachable](#)
- [Releases 4.4.1 and Later—MGW Unreachable, New Call Termination Attempt Occurs](#)

### Release 4.4.0—KA Attempts Unsuccessful, MGW Unreachable

If no ACK is received during any KA attempt, and no MGCP messages have been exchanged between the Cisco BTS 10200 Softswitch and the MGW for a specified time interval (see the time interval description in the drawing), the system performs a specified number of KA retries before declaring the MGW to be unreachable. This condition is shown in [Figure A-10](#).

**Figure A-10** Release 4.4.0—KA Attempts Unsuccessful, MGW Unreachable



190642



#### Note

For detailed examples of successful KA attempts, see [Figure A-1](#) through [Figure A-3](#).

The system takes the following actions in the scenario shown in [Figure A-10](#):

- If KA attempts are successful, and stable calls exist: The system implements the KA pattern shown in Scenario 1. (See [Scenario 1—MGW Reachable](#).)
- For RGWs with 16 or fewer endpoints—If KA attempts are successful, and no stable calls exist: The system implements the KA pattern shown in Scenario 2. (See [Scenario 2 \(Special Case\)—Reachable RGW with 16 or Fewer Endpoints and No Stable Calls In Progress](#).)



**Note**

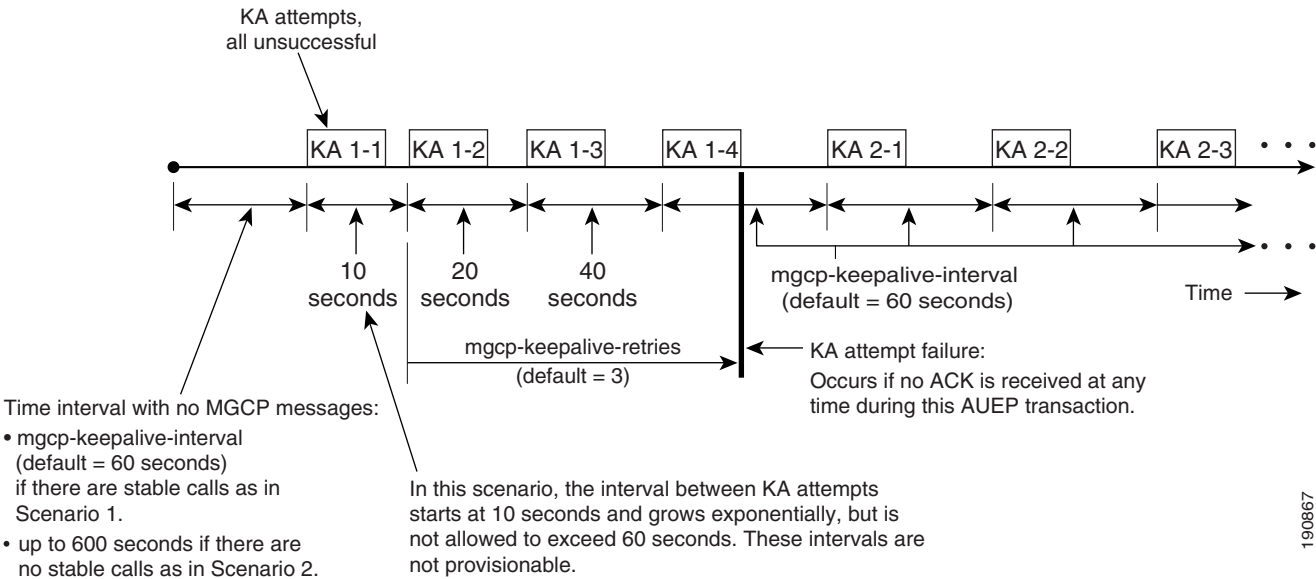
For TGWs and RGWs with more than 16 endpoints—If a KA attempt is successful, the system implements [Scenario 1—MGW Reachable](#) regardless of whether there are stable calls or not.

- If a KA attempt is unsuccessful (Release 4.4.0): The system raises one or more alarms and continues this pattern of KA attempts ([Scenario 3—MGW Unreachable](#)). The system releases any active calls on this MGW. Typical alarms for this condition include:
  - [SIGNALING \(36\)](#)—Trunk locally blocked (applicable to CAS, ISDN, and SS7 trunks)
  - [SIGNALING \(68\)](#)—Media Gateway endpoints are out of service at GW
  - [SIGNALING \(79\)](#)—Media Gateway unreachable
- If all KA attempts are unsuccessful through **mgcp-keepalive-retries**, the system declares the MGW unreachable.

### Releases 4.4.1 and Later—KA Attempts Unsuccessful, MGW Unreachable

If no ACK is received during any KA attempt, and no MGCP messages have been exchanged between the Cisco BTS 10200 Softswitch and the MGW for a specified time interval (see the time interval description in the drawing), the system performs a specified number of KA retries before declaring the MGW to be unreachable. This condition is shown in [Figure A-11](#).

**Figure A-11** Release 4.4.1 Later—KA Attempts Unsuccessful, MGW Unreachable



**Note**

For detailed examples of successful KA attempts, see [Figure A-1](#) through [Figure A-3](#).

The system takes the following actions in the scenario shown in [Figure A-11](#):

- If KA attempts are successful, and stable calls exist: The system implements the KA pattern shown in Scenario 1. (See [Scenario 1—MGW Reachable](#).)
- For RGWs with 16 or fewer endpoints—If KA attempts are successful, and no stable calls exist: The system implements the KA pattern shown in Scenario 2. (See [Scenario 2 \(Special Case\)—Reachable RGW with 16 or Fewer Endpoints and No Stable Calls In Progress](#).)

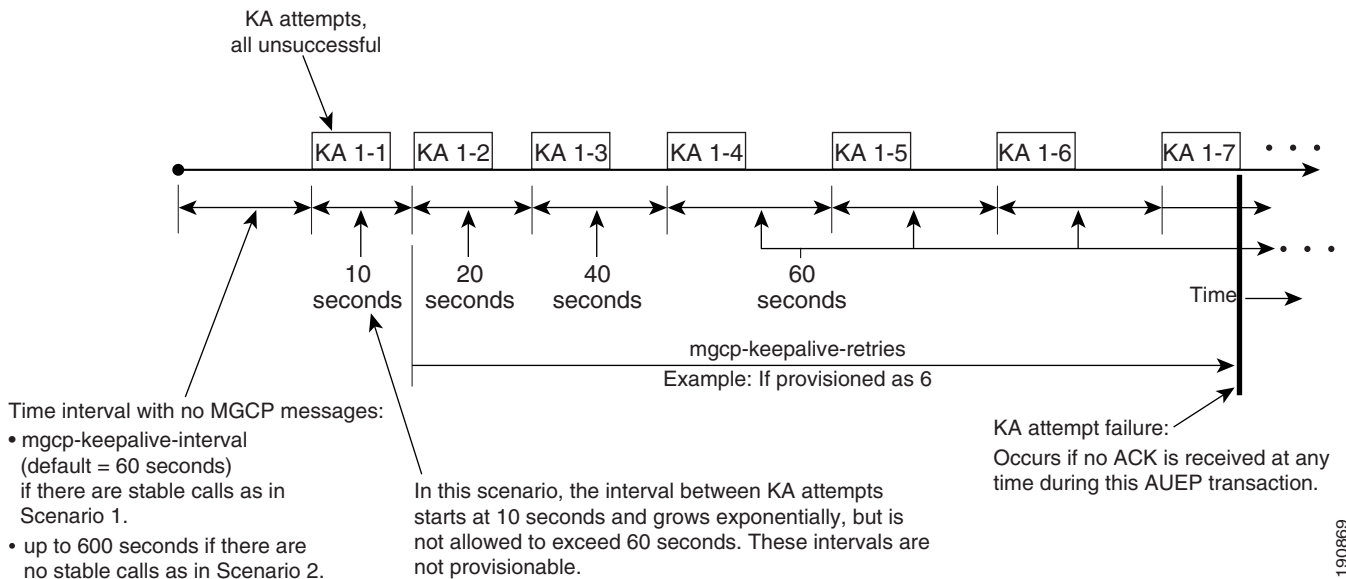
**Note**

For TGWs and RGWs with more than 16 endpoints—If a KA attempt is successful, the system implements [Scenario 1—MGW Reachable](#) regardless of whether there are stable calls or not.

- If a KA attempt is unsuccessful (Release 4.4.1): The system raises one or more alarms and continues this pattern of KA attempts ([Scenario 3—MGW Unreachable](#)). The system does *not* release any active calls on this MGW. Typical alarms for this condition include:
  - [SIGNALING \(36\)](#)—Trunk locally blocked (applicable to CAS, ISDN, and SS7 trunks)
  - [SIGNALING \(68\)](#)—Media Gateway endpoints are out of service at GW
  - [SIGNALING \(79\)](#)—Media Gateway unreachable
- If all KA attempts are unsuccessful through **mgcp-keepalive-retries**, the system declares the MGW unreachable.

[Figure A-12](#) shows an additional example of this condition. In this case the **mgcp-keepalive-retries** token (default = 3) has been provisioned as 6.

**Figure A-12**      **Release 4.4.1 and Later—KA Attempts Unsuccessful, MGW Unreachable**  
(*Illustrative Example with mgcp-keepalive-retries Provisioned as 6*)



190869

## Releases 4.4.1 and Later—MGW Unreachable, New Call Termination Attempt Occurs

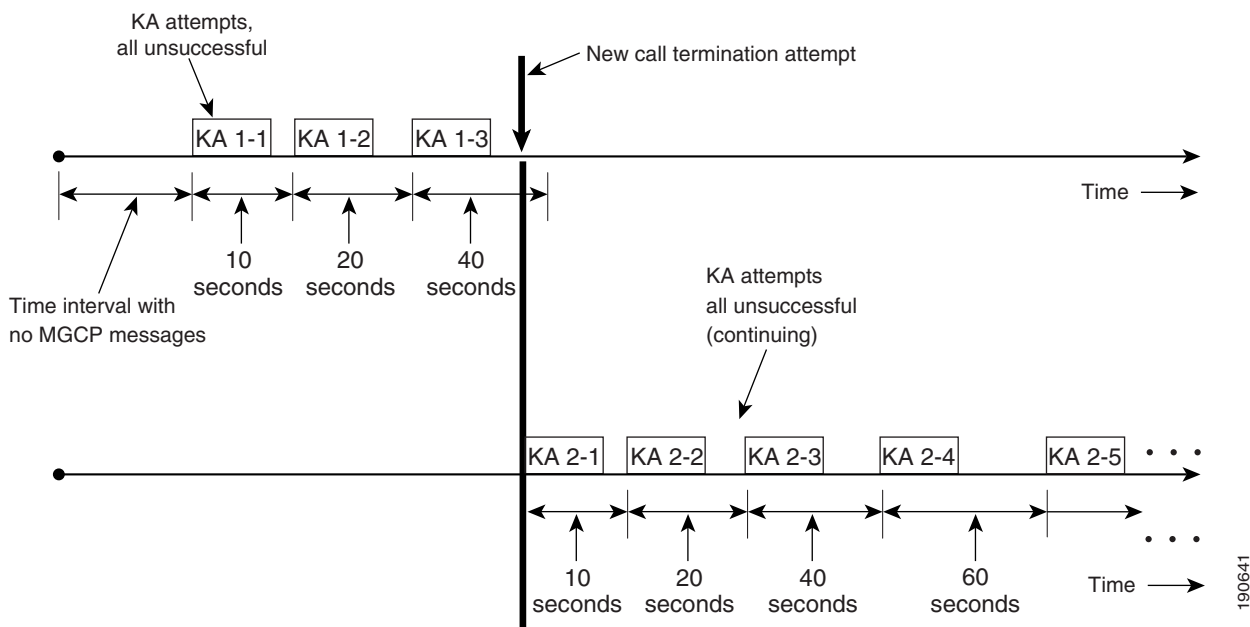
If the MGW is in **down status**, and a new call termination attempt is made on any termination on that MGW, the KA process is expedited even though the next keepalive attempt is scheduled for a later time. If the MGW is still in **down status**, the KA attempts continue. This condition is shown in [Figure A-13](#).



### Note

In this case, the Cisco BTS 10200 Softswitch fails the call immediately after receiving the call termination attempt, without sending any MGCP message to the MGW.

**Figure A-13** Release 4.4.1 and Later—MGW Unreachable, New Call Termination Attempt Occurs







## GLOSSARY

Revised: October 23, 2008, OL-11335-06

### A

|             |                                                    |
|-------------|----------------------------------------------------|
| <b>AAA</b>  | authentication, authorization, and accounting      |
| <b>ACAR</b> | automatic callback and automatic rollback          |
| <b>ACF</b>  | admission confirmation                             |
| <b>ACG</b>  | automatic call gapping                             |
| <b>ACK</b>  | acknowledge                                        |
| <b>ACL</b>  | access control list, automatic congestion level    |
| <b>ACTV</b> | active                                             |
| <b>ADDR</b> | address                                            |
| <b>ADM</b>  | administrative                                     |
| <b>AGGR</b> | aggregation                                        |
| <b>AIN</b>  | Advanced Intelligent Network                       |
| <b>ALT</b>  | alternate                                          |
| <b>ANC</b>  | announcements module                               |
| <b>ANI</b>  | automatic number identification                    |
| <b>ANSI</b> | American National Standards Institute              |
| <b>AOR</b>  | address of record                                  |
| <b>API</b>  | application programming interface                  |
| <b>ARQ</b>  | admission request                                  |
| <b>AS</b>   | application server                                 |
| <b>ASC</b>  | associate                                          |
| <b>ASP</b>  | application service provider                       |
| <b>ATIS</b> | Alliance for Telecommunications Industry Solutions |

**AUCX**                audit connection

**AUEP**                audit endpoint

## **B**

**B8ZS**                binary 8-zero substitution

**BCM**                 Basic Call module

**BDMS**                Bulk Data Management System

**BLG**                 billing

**BLO**                 blocking

**BTS**                 Broadband Telephony Softswitch

**BW**                 band width

## **C**

**CA**                 Call Agent

**CA**                 California

**CALLP**              call processing

**CAS**                channel-associated signaling

**CCB**                call control block

**CCR**                continuity check request

**CCU**                Call Control unit

**CD**                 compact disk

**CDB**                call data block

**CD-ROM**            compact disk - read only media

**CDT**                Central Daylight Time

**CFG**                configuration

**CFN**                confusion

**CGB**                circuit group blocking

**CGU**                circuit group unblocking

|              |                                                                           |
|--------------|---------------------------------------------------------------------------|
| <b>CIC</b>   | circuit identification code, carrier identification code                  |
| <b>CLI</b>   | command line interface                                                    |
| <b>CLLI</b>  | common language location identifier                                       |
| <b>CMJ</b>   | circuit reservation rejected                                              |
| <b>CMTS</b>  | cable modem termination system                                            |
| <b>CNAM</b>  | calling name delivery                                                     |
| <b>CODEC</b> | coder/decoder, compression/decompression                                  |
| <b>COPS</b>  | Common Open Policy Service Protocol                                       |
| <b>CORBA</b> | Common Object Request Broker Architecture                                 |
| <b>COT</b>   | customer-originated trace, continuity testing, central office termination |
| <b>CPE</b>   | customer premises equipment                                               |
| <b>CPU</b>   | central processing unit                                                   |
| <b>CQM</b>   | circuit query message                                                     |
| <b>CQR</b>   | circuit query response                                                    |
| <b>CRC</b>   | cyclic redundancy check                                                   |
| <b>CRCX</b>  | create connection                                                         |
| <b>CS</b>    | capability set (for example, CS-2)                                        |
| <b>CST</b>   | Central Standard Time                                                     |
| <b>CTRL</b>  | control                                                                   |
| <b>CTX</b>   | Centrex                                                                   |
| <b>CVM</b>   | circuit verification message                                              |
| <b>CVR</b>   | circuit verification response                                             |
| <b>CVT</b>   | circuit validation test                                                   |

## D

|             |                                      |
|-------------|--------------------------------------|
| <b>DB</b>   | database                             |
| <b>DBA</b>  | database administrator               |
| <b>DBM</b>  | database management                  |
| <b>DF</b>   | delivery function                    |
| <b>DHCP</b> | Dynamic Host Configuration Protocol  |
| <b>DLCX</b> | delete connection                    |
| <b>DLY</b>  | delay                                |
| <b>DN</b>   | directory number                     |
| <b>DNIS</b> | dialed number identification service |
| <b>DNS</b>  | domain name system                   |
| <b>DOC</b>  | document                             |
| <b>DPC</b>  | destination point code               |
| <b>DSCP</b> | differentiated service code point    |
| <b>DUPU</b> | destination user part unavailable    |

## E

|             |                                    |
|-------------|------------------------------------|
| <b>EA</b>   | equal access                       |
| <b>EGA</b>  | event generator                    |
| <b>EM</b>   | event message                      |
| <b>EMEA</b> | Europe, Middle East, and Asia      |
| <b>EMS</b>  | Element Management System          |
| <b>EP</b>   | endpoint                           |
| <b>EPCF</b> | endpoint connection                |
| <b>ER</b>   | easily recognizable                |
| <b>ESA</b>  | enhanced subscriber authentication |
| <b>ESF</b>  | extended super frame               |

**F**

|              |                                                       |
|--------------|-------------------------------------------------------|
| <b>FAS</b>   | facility associated signaling                         |
| <b>FPGA</b>  | field programmable gate array                         |
| <b>FQDN</b>  | fully qualified domain name                           |
| <b>FS</b>    | Feature Server                                        |
| <b>FSAIN</b> | Feature Server for AIN services                       |
| <b>FSPTC</b> | Feature Server for POTS, Tandem, and Centrex services |
| <b>FTP</b>   | File Transfer Protocol                                |
| <b>FXS</b>   | Foreign Exchange Station                              |

**G**

|            |                              |
|------------|------------------------------|
| <b>GAP</b> | generic address parameter    |
| <b>GB</b>  | gigabits                     |
| <b>GCF</b> | gatekeeper confirmation      |
| <b>GK</b>  | gatekeeper                   |
| <b>GMT</b> | Greenwich Mean Time          |
| <b>GRA</b> | group reset acknowledge      |
| <b>GRJ</b> | gatekeeper reject            |
| <b>GRP</b> | group                        |
| <b>GRQ</b> | gatekeeper request           |
| <b>GRS</b> | group reset                  |
| <b>GTD</b> | generic transport descriptor |
| <b>GTT</b> | global text telephony        |
| <b>GW</b>  | gateway                      |

**H**

|               |                         |
|---------------|-------------------------|
| <b>H323</b>   | H.323 Protocol          |
| <b>H323GW</b> | H323 gateway            |
| <b>H3A</b>    | H.323 signaling adapter |
| <b>HB</b>     | heartbeat               |

**I**

|              |                                     |
|--------------|-------------------------------------|
| <b>IAD</b>   | integrated access device            |
| <b>IAM</b>   | initial address message             |
| <b>ICMP</b>  | Internet Control Message Protocol   |
| <b>ID</b>    | identification                      |
| <b>IDX</b>   | index                               |
| <b>IE</b>    | information element                 |
| <b>IETF</b>  | Internet Engineering Task Force     |
| <b>IN</b>    | intelligent network                 |
| <b>INF</b>   | information                         |
| <b>INFO</b>  | information                         |
| <b>INIT</b>  | initialize                          |
| <b>INR</b>   | information request                 |
| <b>INS</b>   | in service                          |
| <b>IOS</b>   | Integrated Operating System         |
| <b>IP</b>    | Internet Protocol                   |
| <b>IPC</b>   | inter-process communication         |
| <b>IPM</b>   | Internet Protocol Manager           |
| <b>IPSEC</b> | Internet Protocol security          |
| <b>ISDN</b>  | Integrated Services Digital Network |
| <b>ISP</b>   | Internet service provider           |
| <b>ISUP</b>  | ISDN user part                      |

|             |                                 |
|-------------|---------------------------------|
| <b>ITP</b>  | IP transfer point               |
| <b>IVR</b>  | interactive voice response      |
| <b>IXC</b>  | interexchange carrier           |
| <b>J</b>    |                                 |
| <b>JMS</b>  | Java message service            |
| <b>K</b>    |                                 |
| <b>KAM</b>  | keepalive module                |
| <b>KB</b>   | kilobit                         |
| <b>KMS</b>  | Kerberized management server    |
| <b>L</b>    |                                 |
| <b>LAF</b>  | log archive facility            |
| <b>LATA</b> | local access and transport area |
| <b>LBLK</b> | locally blocked                 |
| <b>LIDB</b> | line information database       |
| <b>LNP</b>  | local number portability        |
| <b>LPA</b>  | loop prevention acknowledgement |
| <b>LRN</b>  | local routing number            |
| <b>LSA</b>  | local serving area              |
| <b>M</b>    |                                 |
| <b>M3UA</b> | MTP3 user adapter               |
| <b>MB</b>   | megabit                         |
| <b>MDCX</b> | modify connection               |
| <b>MDL</b>  | message definition language     |
| <b>MGA</b>  | media gateway adapter           |

|             |                                                   |
|-------------|---------------------------------------------------|
| <b>MGCP</b> | Media Gateway Control Protocol                    |
| <b>MGW</b>  | media gateway                                     |
| <b>MIB</b>  | Management Information Base                       |
| <b>MIM</b>  | M3UA Interface Module                             |
| <b>MRMW</b> | multiple readers and multiple writers             |
| <b>ms</b>   | millisecond                                       |
| <b>MTA</b>  | media terminal adapter, Metropolitan Trading Area |
| <b>MTP</b>  | message transfer part                             |
| <b>MTP1</b> | message transfer part 1                           |
| <b>MTP2</b> | message transfer part 2                           |
| <b>MTP3</b> | message transfer part 3                           |
| <b>MTU</b>  | maximum transmission unit                         |

## N

|             |                                                |
|-------------|------------------------------------------------|
| <b>NANP</b> | North American Numbering Plan                  |
| <b>NAS</b>  | network access server                          |
| <b>NCS</b>  | network-based call signaling                   |
| <b>NFAS</b> | non-facility associated signaling              |
| <b>NFS</b>  | network file server                            |
| <b>NIIF</b> | Network Interconnection Interoperability Forum |
| <b>NMS</b>  | network management system                      |
| <b>NNN</b>  | numeric number nomenclature                    |
| <b>NOA</b>  | nature of address                              |
| <b>NPA</b>  | Numbering Plan Area                            |
| <b>NPAC</b> | Number Portability Administration Center       |
| <b>NR</b>   | non-recoverable                                |
| <b>NTP</b>  | Network Time Protocol                          |
| <b>NU</b>   | network unit                                   |



|            |         |
|------------|---------|
| <b>NUM</b> | number  |
| <b>NW</b>  | network |

## O

|             |                                                          |
|-------------|----------------------------------------------------------|
| <b>OAMP</b> | operations, administration, maintenance and provisioning |
| <b>OLI</b>  | originating line information                             |
| <b>OMNI</b> | Ulticom SS7 stack                                        |
| <b>OMS</b>  | OptiCall Messaging System                                |
| <b>OPC</b>  | originating point code                                   |
| <b>OPT</b>  | Open Packet Telephony                                    |
| <b>ORA</b>  | Oracle                                                   |
| <b>OS</b>   | operating system                                         |
| <b>OSS</b>  | operations support system                                |

## P

|             |                                                    |
|-------------|----------------------------------------------------|
| <b>PBX</b>  | private branch exchange                            |
| <b>PDM</b>  | process debug manager                              |
| <b>PDU</b>  | protocol decode unit                               |
| <b>PIC</b>  | presubscribed interexchange carrier, point in call |
| <b>PID</b>  | process ID                                         |
| <b>PMG</b>  | process manager                                    |
| <b>POP</b>  | point of presence                                  |
| <b>POTS</b> | plain old telephone service                        |
| <b>PRI</b>  | primary rate interface                             |
| <b>PSTN</b> | public switched telephone network                  |

**Q**

**QAM** queue processing module

**QoS** quality of service

**QVT** Query Verification Tool

**R**

**RAM** random access memory

**RAS** Registration, Admissions, and Status (signaling function in H.323 for communications to gatekeeper)

**RBLK** remote block

**REL** release

**RFC** request for comment

**RGW** residential gateway

**RKEY** routing key

**RKS** record keeping system

**RLC** release complete

**RMAN** recovery manager

**ROM** read only memory

**RPF** registration and profiling tool

**RQNT** request for notification

**RQNT** notification request

**RR** resource record

**RRJ** request rejected

**RRQ** registration request

**RSC** reset circuit

**RSIP** restart in progress

**RT** re-transact

**RTM** routing module

**RTO** retransmission time out

|             |                                                   |
|-------------|---------------------------------------------------|
| <b>RTP</b>  | Real Time Transport Protocol                      |
| <b>RUDP</b> | Reliable User Datagram Protocol                   |
| <b>RX</b>   | retransmit                                        |
| <b>S</b>    |                                                   |
| <b>S1</b>   | severity 1                                        |
| <b>S2</b>   | severity 2                                        |
| <b>S3</b>   | severity 3                                        |
| <b>S4</b>   | severity 4                                        |
| <b>S7A</b>  | SS7 adapter                                       |
| <b>S7M</b>  | SS7 module                                        |
| <b>SA</b>   | security association                              |
| <b>SAI</b>  | signaling adapter interface                       |
| <b>SAP</b>  | service access point                              |
| <b>SCA</b>  | selective call acceptance, status control adapter |
| <b>SCC</b>  | signaling connection control                      |
| <b>SCCP</b> | signaling connection control part                 |
| <b>SCP</b>  | service control point, signal control point       |
| <b>SCTP</b> | Stream Control Transmission Protocol              |
| <b>SDN</b>  | software defined network                          |
| <b>SFTP</b> | Secure File Transfer Protocol                     |
| <b>SG</b>   | signaling gateway                                 |
| <b>SGP</b>  | signaling gateway process                         |
| <b>SHR</b>  | System Health Report (system-health)              |
| <b>SIA</b>  | SIP adapter                                       |
| <b>SID</b>  | system identification number                      |
| <b>SIP</b>  | Session Initiation Protocol                       |
| <b>SLC</b>  | signaling link code                               |

|             |                                    |
|-------------|------------------------------------|
| <b>SLHR</b> | Service Logic Host Route           |
| <b>SM</b>   | system manager                     |
| <b>SMG</b>  | system manager program             |
| <b>SMS</b>  | service management system          |
| <b>SNMP</b> | Simple Network Management Protocol |
| <b>SP</b>   | service provider                   |
| <b>SQL</b>  | Structured Query Language          |
| <b>SRV</b>  | service                            |
| <b>SS7</b>  | Signaling System 7                 |
| <b>SSH</b>  | secure shell                       |
| <b>SSN</b>  | subsystem number                   |
| <b>SSP</b>  | signal switching point             |
| <b>STP</b>  | signal transfer point              |
| <b>SUA</b>  | SCCP user adapter                  |
| <b>SUB</b>  | subscriber                         |

## T

|                        |                                |
|------------------------|--------------------------------|
| <b>T1</b>              | trunk level 1                  |
| <b>T3</b>              | trunk level 3                  |
| <b>T5</b>              | timer 5                        |
| <b>T13</b>             | timer 13                       |
| <b>T15</b>             | timer 15                       |
| <b>T17</b>             | timer 17                       |
| <b>T19</b>             | timer 19                       |
| <b>T21</b>             | timer 21                       |
| <b>T23</b>             | timer 23                       |
| <b>T28</b>             | timer 28                       |
| <b>T<sub>CCR</sub></b> | timer continuity check request |

|               |                                           |
|---------------|-------------------------------------------|
| <b>TAC</b>    | Technical Assistance Center               |
| <b>TCAP</b>   | Transaction Capabilities Application Part |
| <b>TCP</b>    | Transmission Control Protocol             |
| <b>TDM</b>    | telecommunications data link monitor      |
| <b>TEI</b>    | terminal endpoint identifier              |
| <b>TFC</b>    | transfer controlled                       |
| <b>TG</b>     | trunk group, trunking gateway             |
| <b>TGID</b>   | trunk group ID                            |
| <b>TGN-ID</b> | trunk group ID                            |
| <b>TMM</b>    | Traffic and Measurements module           |
| <b>TOS</b>    | type of service                           |
| <b>TPM</b>    | terminating point master                  |
| <b>TRNS</b>   | transient                                 |
| <b>TSA</b>    | TCAP signaling adapter                    |
| <b>TSAP</b>   | transport service access point            |
| <b>TT</b>     | translation type                          |
| <b>TVT</b>    | Translation Verification Tool             |

## U

|             |                             |
|-------------|-----------------------------|
| <b>UBL</b>  | unblocking message          |
| <b>UDP</b>  | User Datagram Protocol      |
| <b>UEQP</b> | unequipped                  |
| <b>ULP</b>  | Upper Layer Protocol        |
| <b>URI</b>  | uniform resource identifier |
| <b>URL</b>  | universal resource locator  |
| <b>US</b>   | United States               |
| <b>USA</b>  | United States of America    |

## **V**

**VOIP**                      voice over IP

**VTOC**                    volume table of contents

## **W**

## **X**

**XUA**                      extended unit association

**XUDTS**                  extended unit data service

## **Y**

## **Z**