Cisco BTS 10200 Softswitch Troubleshooting Guide, Release 4.5.x

Revised: July 22, 2009

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-8000-32

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.

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at www.cisco.com/go/trademarks. Third party trademarks mentioned 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. (1005R)

Cisco BTS 10200 Softswitch Troubleshooting Guide, Release 4.5.x
Copyright © 2009 Cisco Systems, Inc. All rights reserved.

CONTENTS

Preface xli

Introduction xli

Objective xli

Audience xli

Organization xlii

Conventions xliii

Updates to this Document for Release 4.5.x xliii

New Events and Alarms (Release 3.5 to Release 4.5.1) xlv

Modified Events and Alarms (Release 3.5 to Release 4.5.1) xlix

Deprecated Events and Alarms (Release 4.5 to Release 4.5.1) li

New Events and Alarms (Release 4.5.13 to Release 4.5.1) lii

Modified Events and Alarms (Release 4.5.13 to Release 4.5.1) lii

Deprecated Events and Alarms (Release 4.5.13 to Release 4.5.1) lii

Obtaining Documentation and Submitting a Service Request liii

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 1-17
Format of Events and Alarms 1-18

CHAPTER 2 **Audit Troubleshooting** 2-1
Introduction 2-1
Audit Events and Alarms 2-1
AUDIT (1) 2-2
AUDIT (2) 2-2
AUDIT (3) 2-2
AUDIT (4) 2-3
AUDIT (5) 2-3
AUDIT (6) 2-4
AUDIT (7) 2-4
AUDIT (8) 2-5
AUDIT (9) 2-5
AUDIT (10) 2-6
AUDIT (11) 2-6
AUDIT (12) 2-7
AUDIT (13) 2-7
AUDIT (14) 2-8
AUDIT (15) 2-8
AUDIT (16) 2-9
AUDIT (17) 2-9
AUDIT (18) 2-10
AUDIT (19) 2-10
AUDIT (20) 2-11
Monitoring Audit Events 2-12
Test Report - Audit (1) 2-12
Start or Stop of Signaling System 7 - Circuit Identification Code Audit - Audit (2) 2-12
Signaling System 7 Circuit Identification Code Audit Terminated Before Successful Completion - Audit (3) 2-13
Call Exceeds a Long-Duration Threshold - Audit (4) 2-13
Critical Internal Audit Failure - Audit (5) 2-13
Major Internal Audit Failure - Audit (6) 2-13
Minor Internal Audit Failure - Audit (7) 2-14
Warning From Internal Audit - Audit (8) 2-14

Softswitch Audit SIP CCB Release - Audit (9) 2-14
Memory Audit Complete Status - Audit (10) 2-14
Critical Network Time Protocol Service Failure - Audit (11) 2-14
Major Network Time Protocol Service Failure - Audit (12) 2-14
Minor Network Time Protocol Service Failure - Audit (13) 2-15
Network Time Protocol Service Warning - Audit (14) 2-15
Critical Index Shared Memory Error - Audit (15) 2-15
Process Heap Memory Usage Exceeds Minor Threshold Level - Audit (16) 2-15
Process Heap Memory Usage Exceeds Major Threshold Level - Audit (17) 2-15
Process Heap Memory Usage Exceeds Critical Threshold Level - Audit (18) 2-15
Recovered Memory of Stale Call - Audit (19) 2-16
Audit Found Lost Call Data Record - Audit (20) 2-16
Troubleshooting Audit Alarms 2-17
Critical Internal Audit Failure - Audit (5) 2-17
Major Internal Audit Failure - Audit (6) 2-17
Minor Internal Audit Failure - Audit (7) 2-17
Critical Network Time Protocol Service Failure - Audit (11) 2-18
Major Network Time Protocol Service Failure - Audit (12) 2-18
Minor Network Time Protocol Service Failure - Audit (13) 2-18
Critical Index Shared Memory Error - Audit (15) 2-18
Process Heap Memory Usage Exceeds Minor Threshold Level - Audit (16) 2-18
Process Heap Memory Usage Exceeds Major Threshold Level - Audit (17) 2-18
Process Heap Memory Usage Exceeds Critical Threshold Level - Audit (18) 2-19
Audit Found Lost Call Data Record - Audit (20) 2-19

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 (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
BILLING (60) 3-22
Monitoring Billing Events 3-23
Test Report - Billing (1) 3-24
Billing Partition Disk Usage Minor Threshold Exceeded - Billing (2) 3-24
Billing Partition Disk Usage Major Threshold Exceeded - Billing (3) 3-24
Billing Partition Disk Usage Critical Threshold Exceeded - Billing (4) 3-24
Billing Partition Disk Usage Within Normal Range - Billing (5) 3-24
File Transfer Protocol/Secure File Transfer Protocol Transfer Failed - Billing (6) 3-25
Transmission Control Protocol Connection Error - Billing (7) 3-25
Transmission Control Protocol Packet Receive Failure - Billing (8) 3-25
Database Connection Error - Billing (13) 3-25
File Open Error - Billing (14) 3-25
File Write Error - Billing (15) 3-25
Call Data Block Send Failed - Billing (29) 3-26
Domain Name Mapping Failed - Billing (30) 3-26

Port not Specified - Billing (31) **3-26**
Element Management System Address not Specified - Billing (32) **3-26**
File Transfer Protocol/Secure File Transfer Protocol Parameters Invalid - Billing (33) **3-26**
All Billing Links at Billing Server Down - Billing (35) **3-26**
Billing Link Restored - Billing (36) **3-27**
Billing Link Failure - Billing (37) **3-27**
Event Message Log File Access Error - Billing (38) **3-27**
Event Message Encode Failure - Billing (40) **3-27**
Message Content Error - Billing (41) **3-27**
Error Reading Provisioned Data–Using Default - Billing (42) **3-27**
Record Keeping System Switch Occurred - Billing (44) **3-27**
Event Message Log File Opened - Billing (45) **3-28**
Event Message Log File Closed - Billing (46) **3-28**
Record Keeping System Unreachable for One Hour - Billing (47) **3-28**
Record Keeping System Unreachable for Three Hours - Billing (48) **3-28**
Record Keeping System Unreachable for Five Hours - Billing (49) **3-28**
Bulk Data Management System Stopped Generating New Billing File - Billing (52) **3-28**
Event Message Disk Space 50 Percent Full - Billing (53) **3-29**
Event Message Disk Space 70 Percent Full - Billing (54) **3-29**
Event Message Disk Space 100 Percent Full - Billing (55) **3-29**
Billing Data Corruption Detected - Billing (56) **3-29**
Prepaid Subscriber Call Attempt Failed Because of Balance - Billing (57) **3-29**
Signaling Prepaid Server Inaccessible - Billing (58) **3-29**
Bad File Detected During Startup - Billing (60) **3-30**
Troubleshooting Billing Alarms **3-31**
Billing Partition Disk Usage Minor Threshold Exceeded - Billing (2) **3-32**
Billing Partition Disk Usage Major Threshold Exceeded - Billing (3) **3-32**
Billing Partition Disk Usage Critical Threshold Exceeded - Billing (4) **3-32**
File Transfer Protocol/Secure File Transfer Protocol Transfer Failed - Billing (6) **3-33**
Transmission Control Protocol Connection Error - Billing (7) **3-34**
Transmission Control Protocol Packet Receive Failure - Billing (8) **3-34**
Database Connection Error - Billing (13) **3-34**
File Write Error - Billing (15) **3-34**
Call Data Block Send Failed - Billing (29) **3-35**
Domain Name Mapping Failed - Billing (30) **3-35**
Port not Specified - Billing (31) **3-35**
Element Management System Address not Specified - Billing (32) **3-35**
File Transfer Protocol/Secure File Transfer Protocol Parameters Invalid - Billing (33) **3-35**
All Billing Links at Billing Server Down - Billing (35) **3-36**
Billing Link Failure - Billing (37) **3-36**

Event Message Log File Access Error - Billing (38) 3-36
Event Message Encode Failure - Billing (40) 3-36
Message Content Error - Billing (41) 3-36
Record Keeping System Switch Occurred - Billing (44) 3-37
Event Message Log File Opened - Billing (45) 3-37
Event Message Log File Closed - Billing (46) 3-37
Record Keeping System Unreachable for One Hour - Billing (47) 3-37
Record Keeping System Unreachable for Three Hours - Billing (48) 3-37
Record Keeping System Unreachable for 5 Hours - Billing (49) 3-38
Bulk Data Management System Stopped Generating New Billing File - Billing (52) 3-38
Event Message Disk Space 50 Percent Full - Billing (53) 3-38
Event Message Disk Space 70 Percent Full - Billing (54) 3-38
Event Message Disk Space 100 Percent Full - Billing (55) 3-38
Billing Data Corruption Detected - Billing (56) 3-39
Signaling Prepaid Server Inaccessible - Billing (58) 3-39
Bad File Detected During Startup - Billing (60) 3-39

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
CALLP (40) 4-19
CALLP (41) 4-19
Monitoring Call Processing Events 4-20
Test Report - Call Processing (1) 4-21
No Route Available for Called Number - Call Processing (8) 4-21
No Route Available for Carrier Dialed - Call Processing (9) 4-21
Feature Server One Link Down - Call Processing (11) 4-21
Feature Server Both Links Down - Call Processing (12) 4-22
Network Access Server Create Connection Error - Call Processing (13) 4-22
Network Access Server Authentication Failure - Call Processing (14) 4-22
Cable Modem Termination System Easily Recognizable Identification Not Found in Media Gateway Table - Call Processing (15) 4-22
Route Index has No Trunk Group Assigned - Call Processing (16) 4-22
Invalid Route Index Used - Call Processing (17) 4-22
Unable to Play Announcement - Call Processing (18) 4-23
Call Routed to Unprovisioned Subscriber - Call Processing (19) 4-23
No Route or Trunk Group Available to Route Call - Call Processing (20) 4-23
Call Released Due to Maximum Hop Counts Exceeded - Call Processing (21) 4-23
Trunk Group Index Read Failure - Call Processing (22) 4-23
Routing Error: Termination is Not a Subscriber - Call Processing (23) 4-23
Invalid Route for Subscriber Index - Call Processing (24) 4-24
Invalid Route Group for Subscriber Routing - Call Processing (25) 4-24
Invalid Trunk Group for Subscriber Routing - Call Processing (26) 4-24
Unable to Route: Blocked by Destination Subscriber Status - Call Processing (27) 4-24
Route Name Does Not Exist - Call Processing (28) 4-24
Routing Selection Failure - Call Processing (29) 4-24
Customer-Originated Trace Test Failed - Call Processing (30) 4-25

Call Authorization Failure - Call Processing (31) 4-25
Country Code Dialing Plan Error - Call Processing (32) 4-25
Invalid Call - Call Processing (33) 4-25
Dial Plan Information Not Found for Digits Received - Call Processing (34) 4-25
Dial Plan Information for Test Call Not Found - Call Processing (35) 4-25
Invalid or Unknown Nature of Address - Call Processing (36) 4-26
Call Failure - Call Processing (37) 4-26
Release Cause 25 Exchange Routing Error Received - Call Processing (38) 4-26
Test Call Blocked Due to Congestion or Isolation - Call Processing (39) 4-26
Interactive Voice Response Real Time Transport Protocol Session Fail - Call Processing (40) 4-26
INVITE Message From Unauthorized Call Agent - Call Processing (41) 4-26
Troubleshooting Call Processing Alarms 4-27
Feature Server One Link Down - Call Processing (11) 4-27
Feature Server Both Links Down - Call Processing (12) 4-29
Release Cause 25 Exchange Routing Error Received - Call Processing (38) 4-30
INVITE Message From Unauthorized Call Agent - Call Processing (41) 4-30

CHAPTER 5 **Configuration Troubleshooting** 5-1
Introduction 5-1
Configuration Events and Alarms 5-1
CONFIG (1) 5-2
CONFIG (2) 5-2
CONFIG (3) 5-3
CONFIG (4) 5-3
CONFIG (5) 5-4
Monitoring Configuration Events 5-5
Test Report - Configuration (1) 5-5
Signaling Media Gateway Adapter Wrongly Configured Domain Name - Configuration (2) 5-5
Mate Configuration Error - Configuration (3) 5-5
Configuration Error - Configuration (4) 5-5
Feature-Server Database and Command Line Host Mismatch - Configuration (5) 5-6
Troubleshooting Configuration Alarms 5-7
Mate Configuration Error - Configuration (3) 5-7
Configuration Error - Configuration (4) 5-7
Feature-Server Database and Command Line Host Mismatch - Configuration (5) 5-7

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) 6-7
DATABASE (9) 6-8
DATABASE (10) 6-8
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
DATABASE (21) 6-15
DATABASE (25) 6-16
DATABASE (26) 6-16

Monitoring Database Events 6-17

Test Report - Database (1) 6-17
Database Management Update Failure: Master/Slave Database Out of Sync - Database (2) 6-18
There are Errors in Element Management System Database DefError Queue; Contact Database Administrator - Database (3) 6-18
Element Management System Database HeartBeat: Replication PUSH Job Broken - Database (4) 6-18
Element Management System Database HeartBeat Process Died - Database (5) 6-18
Element Management System Database Replication DefTranDest Queue Overloaded - Database (6) 6-18
Element Management System Database DefTran Queue is Overloaded - Database (7) 6-19
Element Management System Database Tablespace is Out of Free Space - Database (8) 6-19
Urgent: Element Management System Database Archive Log Directory is Getting Full - Database (9) 6-19
Element Management System Database: Backup Fails - Database (10) 6-19
Element Management System Database Alert.log Alerts - Database (11) 6-19
Element Management System Database Process Died - Database (12) 6-19

Element Management System Database Performance Alert - Database (13) 6-20
Table Size Exceeds Minor Threshold Limit - Database (14) 6-20
Table Size Exceeds Major Threshold Limit - Database (15) 6-20
Table Size Exceeds Critical Threshold Limit - Database (16) 6-20
Data Replication Failed - Database (17) 6-20
Unexpected Runtime Data Interaction - Database (18) 6-20
Daily Database Backup Completed Successfully - Database (19) 6-21
Replication Data Flush Timeout During Switchover - Database (20) 6-21
Database Statistics Collection Exception - Database (21) 6-21
Secure File Transfer Protocol Transfer Failed—Database (25) 6-21
File Write Error—Database (26) 6-21
Troubleshooting Database Alarms 6-22
There Are Errors in Element Management System Database DefError Queue; Contact Database Administrator - Database (3) 6-23
Element Management System Database HeartBeat: Replication PUSH Job Broken - Database (4) 6-23
Element Management System Database HeartBeat Process Died - Database (5) 6-23
Element Management System Database Replication DefTranDest Queue Overloaded - Database (6) 6-24
Element Management System Database DefTran Queue is Overloaded - Database (7) 6-24
Element Management System Database Tablespace is Out of Free Space - Database (8) 6-24
Urgent: Element Management System Database Archive Log Directory is Getting Full - Database (9) 6-24
Element Management System Database: Backup Fails - Database (10) 6-24
Element Management System Database Alert.log Alerts - Database (11) 6-25
Element Management System Database Process Died - Database (12) 6-25
Element Management System Database Performance Alert - Database (13) 6-25
Table Size Exceeds Minor Threshold Limit - Database (14) 6-26
Table Size Exceeds Major Threshold Limit - Database (15) 6-26
Table Size Exceeds Critical Threshold Limit - Database (16) 6-26
Data Replication Failed - Database (17) 6-26
Replication Data Flush Timeout During Switchover - Database (20) 6-26
Database Statistics Collection Exception - Database (21) 6-26
Secure File Transfer Protocol Transfer Failed—Database (25) 6-27
File Write Error—Database (26) 6-27

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

MAINTENANCE (43) 7-26
MAINTENANCE (44) 7-26
MAINTENANCE (45) 7-27
MAINTENANCE (46) 7-27
MAINTENANCE (47) 7-28
MAINTENANCE (48) 7-28
MAINTENANCE (49) 7-29
MAINTENANCE (50) 7-29
MAINTENANCE (51) 7-30
MAINTENANCE (52) 7-30
MAINTENANCE (53) 7-31
MAINTENANCE (54) 7-31
MAINTENANCE (55) 7-32
MAINTENANCE (56) 7-32
MAINTENANCE (57) 7-33
MAINTENANCE (58) 7-34
MAINTENANCE (61) 7-35
MAINTENANCE (62) 7-35
MAINTENANCE (63) 7-36
MAINTENANCE (64) 7-36
MAINTENANCE (65) 7-37
MAINTENANCE (66) 7-37
MAINTENANCE (67) 7-38
MAINTENANCE (68) 7-38
MAINTENANCE (69) 7-39
MAINTENANCE (70) 7-39
MAINTENANCE (71) 7-40
MAINTENANCE (72) 7-40
MAINTENANCE (73) 7-41
MAINTENANCE (74) 7-41
MAINTENANCE (75) 7-42
MAINTENANCE (77) 7-42
MAINTENANCE (78) 7-43
MAINTENANCE (79) 7-43
MAINTENANCE (80) 7-44
MAINTENANCE (81) 7-44
MAINTENANCE (82) 7-45
MAINTENANCE (83) 7-45
MAINTENANCE (84) 7-46
MAINTENANCE (85) 7-46

MAINTENANCE (86) 7-47
MAINTENANCE (87) 7-47
MAINTENANCE (88) 7-48
MAINTENANCE (89) 7-48
MAINTENANCE (90) 7-49
MAINTENANCE (91) 7-49
MAINTENANCE (92) 7-50
MAINTENANCE (93) 7-50
MAINTENANCE (94) 7-51
MAINTENANCE (95) 7-51
MAINTENANCE (96) 7-52
MAINTENANCE (97) 7-52
MAINTENANCE (98) 7-53
MAINTENANCE (99) 7-53
MAINTENANCE (100) 7-54
MAINTENANCE (101) 7-54
MAINTENANCE (102) 7-55
MAINTENANCE (103) 7-55
MAINTENANCE (104) 7-56
MAINTENANCE (105) 7-56
MAINTENANCE (106) 7-57
MAINTENANCE (107) 7-57
MAINTENANCE (108) 7-58
MAINTENANCE (109) 7-58
MAINTENANCE (110) 7-59
MAINTENANCE (111) 7-59
MAINTENANCE (118) 7-60
MAINTENANCE (119) 7-60
MAINTENANCE (120) 7-61
MAINTENANCE (122) 7-62
MAINTENANCE (123) 7-62
Monitoring Maintenance Events 7-63
Test Report - Maintenance (1) 7-66
Report Threshold Exceeded - Maintenance (2) 7-66
Local Side has Become Faulty - Maintenance (3) 7-67
Mate Side has Become Faulty - Maintenance (4) 7-67
Changeover Failure - Maintenance (5) 7-67
Changeover Timeout - Maintenance (6) 7-67
Mate Rejected Changeover - Maintenance (7) 7-67
Mate Changeover Timeout - Maintenance (8) 7-67

Local Initialization Failure - Maintenance (9) **7-67**
Local Initialization Timeout - Maintenance (10) **7-68**
Switchover Complete - Maintenance (11) **7-68**
Initialization Successful - Maintenance (12) **7-68**
Administrative State Change - Maintenance (13) **7-68**
Call Agent Administrative State Change - Maintenance (14) **7-68**
Feature Server Administrative State Change - Maintenance (15) **7-68**
Process Manager: Starting Process - Maintenance (16) **7-68**
Invalid Event Report Received - Maintenance (17) **7-69**
Process Manager: Process has Died - Maintenance (18) **7-69**
Process Manager: Process Exceeded Restart Rate - Maintenance (19) **7-69**
Lost Connection to Mate - Maintenance (20) **7-69**
Network Interface Down - Maintenance (21) **7-69**
Mate is Alive - Maintenance (22) **7-69**
Process Manager: Process Failed to Complete Initialization - Maintenance (23) **7-70**
Process Manager: Restarting Process - Maintenance (24) **7-70**
Process Manager: Changing State - Maintenance (25) **7-70**
Process Manager: Going Faulty - Maintenance (26) **7-70**
Process Manager: Changing Over to Active - Maintenance (27) **7-70**
Process Manager: Changing Over to Standby - Maintenance (28) **7-70**
Administrative State Change Failure - Maintenance (29) **7-71**
Element Manager State Change - Maintenance (30) **7-71**
Process Manager: Sending Go Active to Process - Maintenance (32) **7-71**
Process Manager: Sending Go Standby to Process - Maintenance (33) **7-71**
Process Manager: Sending End Process to Process - Maintenance (34) **7-71**
Process Manager: All Processes Completed Initialization - Maintenance (35) **7-71**
Process Manager: Sending All Processes Initialization Complete to Process - Maintenance (36) **7-72**
Process Manager: Killing Process - Maintenance (37) **7-72**
Process Manager: Clearing the Database - Maintenance (38) **7-72**
Process Manager: Cleared the Database - Maintenance (39) **7-72**
Process Manager: Binary Does not Exist for Process - Maintenance (40) **7-72**
Administrative State Change Successful with Warning - Maintenance (41) **7-72**
Number of Heartbeat Messages Received is Less Than 50% of Expected - Maintenance (42) **7-73**
Process Manager: Process Failed to Come Up in Active Mode - Maintenance (43) **7-73**
Process Manager: Process Failed to Come Up in Standby Mode - Maintenance (44) **7-73**
Application Instance State Change Failure - Maintenance (45) **7-73**
Network Interface Restored - Maintenance (46) **7-73**
Thread Watchdog Counter Expired for a Thread - Maintenance (47) **7-73**
Index Table Usage Exceeded Minor Usage Threshold Level - Maintenance (48) **7-74**
Index Table Usage Exceeded Major Usage Threshold Level - Maintenance (49) **7-74**

Index Table Usage Exceeded Critical Usage Threshold Level - Maintenance (50) 7-74
A Process Exceeds 70% of Central Processing Unit Usage - Maintenance (51) 7-74
Central Processing Unit Usage is Now Below the 50% Level - Maintenance (52) 7-74
The Central Processing Unit Usage is Over 90% Busy - Maintenance (53) 7-74
The Central Processing Unit has Returned to Normal Levels of Operation - Maintenance (54) 7-75
The Five Minute Load Average is Abnormally High - Maintenance (55) 7-75
The Load Average has Returned to Normal Levels - Maintenance (56) 7-75
Memory and Swap are Consumed at Critical Levels - Maintenance (57) 7-75
Memory and Swap are Consumed at Abnormal Levels - Maintenance (58) 7-75
No Heartbeat Messages Received Through the Interface - Maintenance (61) 7-76
Link Monitor: Interface Lost Communication - Maintenance (62) 7-76
Outgoing Heartbeat Period Exceeded Limit - Maintenance (63) 7-76
Average Outgoing Heartbeat Period Exceeds Major Alarm Limit - Maintenance (64) 7-76
Disk Partition Critically Consumed - Maintenance (65) 7-76
Disk Partition Significantly Consumed - Maintenance (66) 7-76
The Free Inter-Process Communication Pool Buffers Below Minor Threshold - Maintenance (67) 7-77
The Free Inter-Process Communication Pool Buffers Below Major Threshold - Maintenance (68) 7-77
The Free Inter-Process Communication Pool Buffers Below Critical Threshold - Maintenance (69) 7-77
The Free Inter-Process Communication Pool Buffer Count Below Minimum Required - Maintenance (70) 7-77
Local Domain Name System Server Response Too Slow - Maintenance (71) 7-77
External Domain Name System Server Response Too Slow - Maintenance (72) 7-78
External Domain Name System Server not Responsive - Maintenance (73) 7-78
Local Domain Name System Service not Responsive - Maintenance (74) 7-78
Mismatch of Internet Protocol Address Local Server and Domain Name System - Maintenance (75) 7-78
Mate Time Differs Beyond Tolerance - Maintenance (77) 7-78
Bulk Data Management System Admin State Change - Maintenance (78) 7-78
Resource Reset - Maintenance (79) 7-79
Resource Reset Warning - Maintenance (80) 7-79
Resource Reset Failure - Maintenance (81) 7-79
Average Outgoing Heartbeat Period Exceeds Critical Limit - Maintenance (82) 7-79
Swap Space Below Minor Threshold - Maintenance (83) 7-79
Swap Space Below Major Threshold - Maintenance (84) 7-79
Swap Space Below Critical Threshold - Maintenance (85) 7-79
System Health Report Collection Error - Maintenance (86) 7-80
Status Update Process Request Failed - Maintenance (87) 7-80
Status Update Process Database List Retrieval Error - Maintenance (88) 7-80

Status Update Process Database Update Error - Maintenance (89) **7-80**
Disk Partition Moderately Consumed - Maintenance (90) **7-80**
Internet Protocol Manager Configuration File Error - Maintenance (91) **7-80**
Internet Protocol Manager Initialization Error - Maintenance (92) **7-81**
Internet Protocol Manager Interface Failure - Maintenance (93) **7-81**
Internet Protocol Manager Interface State Change - Maintenance (94) **7-81**
Internet Protocol Manager Interface Created - Maintenance (95) **7-81**
Internet Protocol Manager Interface Removed - Maintenance (96) **7-81**
Inter-Process Communication Input Queue Entered Throttle State - Maintenance (97) **7-81**
Inter-Process Communication Input Queue Depth at 25% of its Hi-Watermark - Maintenance (98) **7-82**
Inter-Process Communication Input Queue Depth at 50% of its Hi-Watermark - Maintenance (99) **7-82**
Inter-Process Communication Input Queue Depth at 75% of its Hi-Watermark - Maintenance (100) **7-82**
Switchover in Progress - Maintenance (101) **7-82**
Thread Watchdog Counter Close to Expiry for a Thread - Maintenance (102) **7-82**
Central Processing Unit is Offline - Maintenance (103) **7-83**
Aggregration Device Address Successfully Resolved - Maintenance (104) **7-83**
Unprovisioned Aggregration Device Detected - Maintenance (105) **7-83**
Aggregration Device Address Resolution Failure - Maintenance (106) **7-83**
No Heartbeat Messages Received Through Interface From Router - Maintenance (107) **7-83**
A Log File Cannot be Transferred - Maintenance (108) **7-83**
Five Successive Log Files Cannot be Transferred - Maintenance (109) **7-84**
Access to Log Archive Facility Configuration File Failed or File Corrupted - Maintenance (110) **7-84**
Cannot Login to External Archive Server - Maintenance (111) **7-84**
Domain Name Server Zone Database does not Match Between the Primary Domain Name Server and the Internal Secondary Authoritative Domain Name Server - Maintenance (118) **7-84**
Periodic Shared Memory Database Backup Failure - Maintenance (119) **7-84**
Periodic Shared Memory Database Backup Success - Maintenance (120) **7-85**
Northbound Provisioning Message is Retransmitted - Maintenance (122) **7-85**
Northbound Provisioning Message Dropped Due To Full Index Table - Maintenance (123) **7-85**
Troubleshooting Maintenance Alarms **7-86**
Local Side has Become Faulty - Maintenance (3) **7-88**
Mate Side has Become Faulty - Maintenance (4) **7-88**
Changeover Failure - Maintenance (5) **7-89**
Changeover Timeout - Maintenance (6) **7-89**
Mate Rejected Changeover - Maintenance (7) **7-89**
Mate Changeover Timeout - Maintenance (8) **7-92**
Local Initialization Failure - Maintenance (9) **7-92**

Local Initialization Timeout - Maintenance (10) **7-92**
Process Manager: Process has Died - Maintenance (18) **7-92**
Process Manager: Process Exceeded Restart Rate - Maintenance (19) **7-92**
Lost Connection to Mate - Maintenance (20) **7-93**
Network Interface Down - Maintenance (21) **7-93**
Process Manager: Process Failed to Complete Initialization - Maintenance (23) **7-93**
Process Manager: Restarting Process - Maintenance (24) **7-93**
Process Manager: Going Faulty - Maintenance (26) **7-93**
Process Manager: Binary Does not Exist for Process - Maintenance (40) **7-94**
Number of Heartbeat Messages Received is Less Than 50% of Expected - Maintenance (42) **7-94**
Process Manager: Process Failed to Come Up in Active Mode - Maintenance (43) **7-94**
Process Manager: Process Failed to Come Up in Standby Mode - Maintenance (44) **7-94**
Application Instance State Change Failure - Maintenance (45) **7-94**
Thread Watchdog Counter Expired for a Thread - Maintenance (47) **7-95**
Index Table Usage Exceeded Minor Usage Threshold Level - Maintenance (48) **7-96**
Index Table Usage Exceeded Major Usage Threshold Level - Maintenance (49) **7-96**
Index Table Usage Exceeded Critical Usage Threshold Level - Maintenance (50) **7-96**
A Process Exceeds 70% of Central Processing Unit Usage - Maintenance (51) **7-96**
The Central Processing Unit Usage is Over 90% Busy - Maintenance (53) **7-96**
The Five Minute Load Average is Abnormally High - Maintenance (55) **7-97**
Memory and Swap are Consumed at Critical Levels - Maintenance (57) **7-97**
No Heartbeat Messages Received Through the Interface - Maintenance (61) **7-97**
Link Monitor: Interface Lost Communication - Maintenance (62) **7-97**
Outgoing Heartbeat Period Exceeded Limit - Maintenance (63) **7-98**
Average Outgoing Heartbeat Period Exceeds Major Alarm Limit - Maintenance (64) **7-98**
Disk Partition Critically Consumed - Maintenance (65) **7-98**
Disk Partition Significantly Consumed - Maintenance (66) **7-98**
The Free Inter-Process Communication Pool Buffers Below Minor Threshold - Maintenance (67) **7-98**
The Free Inter-Process Communication Pool Buffers Below Major Threshold - Maintenance (68) **7-99**
The Free Inter-Process Communication Pool Buffers Below Critical Threshold - Maintenance (69) **7-99**
The Free Inter-Process Communication Pool Buffer Count Below Minimum Required - Maintenance (70) **7-99**
Local Domain Name System Server Response Too Slow - Maintenance (71) **7-99**
External Domain Name System Server Response Too Slow - Maintenance (72) **7-99**
External Domain Name System Server not Responsive - Maintenance (73) **7-100**
Local Domain Name System Service not Responsive - Maintenance (74) **7-100**
Mate Time Differs Beyond Tolerance - Maintenance (77) **7-100**
Average Outgoing Heartbeat Period Exceeds Critical Limit - Maintenance (82) **7-100**

Swap Space Below Minor Threshold - Maintenance (83) **7-100**
Swap Space Below Major Threshold - Maintenance (84) **7-101**
Swap Space Below Critical Threshold - Maintenance (85) **7-101**
System Health Report Collection Error - Maintenance (86) **7-101**
Status Update Process Request Failed - Maintenance (87) **7-101**
Status Update Process Database List Retrieval Error - Maintenance (88) **7-101**
Status Update Process Database Update Error - Maintenance (89) **7-101**
Disk Partition Moderately Consumed - Maintenance (90) **7-102**
Internet Protocol Manager Configuration File Error - Maintenance (91) **7-102**
Internet Protocol Manager Initialization Error - Maintenance (92) **7-102**
Internet Protocol Manager Interface Failure - Maintenance (93) **7-102**
Inter-Process Communication Input Queue Entered Throttle State - Maintenance (97) **7-102**
Inter-Process Communication Input Queue Depth at 25% of Its Hi-Watermark - Maintenance (98) **7-102**
Inter-Process Communication Input Queue Depth at 50% of Its Hi-Watermark - Maintenance (99) **7-103**
Inter-Process Communication Input Queue Depth at 75% of Its Hi-Watermark - Maintenance (100) **7-103**
Switchover in Progress - Maintenance (101) **7-103**
Thread Watchdog Counter Close to Expiry for a Thread - Maintenance (102) **7-103**
Central Processing Unit is Offline - Maintenance (103) **7-104**
No Heartbeat Messages Received Through Interface From Router - Maintenance (107) **7-104**
Five Successive Log Files Cannot be Transferred - Maintenance (109) **7-104**
Access to Log Archive Facility Configuration File Failed or File Corrupted - Maintenance (110) **7-104**
Cannot Login to External Archive Server - Maintenance (111) **7-104**
Domain Name Server Zone Database does not Match Between the Primary Domain Name Server and the Internal Secondary Authoritative Domain Name Server - Maintenance (118) **7-105**
Periodic Shared Memory Database Backup Failure - Maintenance (119) **7-105**

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) 8-7
Monitoring Operations Support System Events 8-8
Test Report - Operations Support System (1) 8-8
Undefined Variable in Known Set - Operations Support System (2) 8-8
Undefined Data Column Identification - Operations Support System (3) 8-8
Request Handler Instantiation Error - Operations Support System (4) 8-9
Structured Query Language Error While Getting Statistics - Operations Support System (5) 8-9
Structured Query Language Connection Error - Operations Support System (6) 8-9
Simple Network Management Protocol File Read Error - Operations Support System (7) 8-9
No Reply Received from Destination - Operations Support System (8) 8-9
Simple Network Management Protocol Authentication Error - Operations Support System (9) 8-9
Queue Processing Module Database Management Index Failed with Error - Operations Support System (10) 8-10
Queue Processing Module Database Management Index Mismatch During Add or Delete - Operations Support System (11) 8-10
Troubleshooting Operations Support System Alarms 8-11
Undefined Variable in Known Set - Operations Support System (2) 8-11
Undefined Data Column Identification - Operations Support System (3) 8-11
Request Handler Instantiation Error - Operations Support System (4) 8-11
Structured Query Language Error While Getting Statistics - Operations Support System (5) 8-12
Structured Query Language Connection Error - Operations Support System (6) 8-12
No Reply Received from Destination - Operations Support System (8) 8-12
Simple Network Management Protocol Authentication Error - Operations Support System (9) 8-12
Queue Processing Module Database Management Index Failed with Error - Operations Support System (10) 8-13

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
SECURITY (6) 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
Secure Session Initiation Protocol Endpoint Validation Failure - Security (6) 9-6
Troubleshooting Security Alarms 9-6
Internet Protocol Security Connection Down - Security (3) 9-6

CHAPTER 10 **Signaling Troubleshooting** 10-1
Introduction 10-1
Signaling Events and Alarms 10-2
SIGNALING (1) 10-3
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) 10-24
SIGNALING (42) 10-25
SIGNALING (43) 10-25
SIGNALING (44) 10-26
SIGNALING (45) 10-26
SIGNALING (46) 10-27
SIGNALING (49) 10-27
SIGNALING (50) 10-28
SIGNALING (51) 10-28
SIGNALING (52) 10-29
SIGNALING (53) 10-29
SIGNALING (54) 10-30
SIGNALING (55) 10-30
SIGNALING (57) 10-31
SIGNALING (58) 10-31
SIGNALING (59) 10-32
SIGNALING (60) 10-32
SIGNALING (61) 10-33
SIGNALING (62) 10-33
SIGNALING (63) 10-34
SIGNALING (64) 10-34
SIGNALING (65) 10-35
SIGNALING (66) 10-35
SIGNALING (68) 10-36
SIGNALING (69) 10-36
SIGNALING (70) 10-37
SIGNALING (71) 10-37
SIGNALING (72) 10-38
SIGNALING (73) 10-38
SIGNALING (74) 10-39
SIGNALING (75) 10-39
SIGNALING (76) 10-40
SIGNALING (77) 10-40
SIGNALING (78) 10-41
SIGNALING (79) 10-41
SIGNALING (80) 10-42
SIGNALING (81) 10-42

SIGNALING (82) 10-43
SIGNALING (83) 10-43
SIGNALING (84) 10-44
SIGNALING (85) 10-44
SIGNALING (86) 10-45
SIGNALING (87) 10-45
SIGNALING (88) 10-46
SIGNALING (89) 10-46
SIGNALING (90) 10-47
SIGNALING (91) 10-47
SIGNALING (92) 10-48
SIGNALING (93) 10-48
SIGNALING (94) 10-49
SIGNALING (95) 10-49
SIGNALING (96) 10-50
SIGNALING (97) 10-50
SIGNALING (98) 10-51
SIGNALING (99) 10-51
SIGNALING (100) 10-52
SIGNALING (101) 10-52
SIGNALING (102) 10-53
SIGNALING (103) 10-53
SIGNALING (104) 10-54
SIGNALING (105) 10-54
SIGNALING (106) 10-55
SIGNALING (107) 10-56
SIGNALING (108) 10-57
SIGNALING (109) 10-57
SIGNALING (110) 10-58
SIGNALING (111) 10-58
SIGNALING (112) 10-59
SIGNALING (113) 10-59
SIGNALING (114) 10-60
SIGNALING (115) 10-60
SIGNALING (116) 10-61
SIGNALING (117) 10-61
SIGNALING (118) 10-62
SIGNALING (119) 10-62
SIGNALING (120) 10-63
SIGNALING (121) 10-63

SIGNALING (122) 10-64
SIGNALING (124) 10-64
SIGNALING (125) 10-65
SIGNALING (126) 10-65
SIGNALING (127) 10-65
SIGNALING (132) 10-66
SIGNALING (133) 10-66
SIGNALING (134) 10-67
SIGNALING (135) 10-67
SIGNALING (136) 10-68
SIGNALING (137) 10-69
SIGNALING (138) 10-69
SIGNALING (139) 10-70
SIGNALING (140) 10-70
SIGNALING (141) 10-71
SIGNALING (142) 10-71
SIGNALING (143) 10-72
SIGNALING (144) 10-72
SIGNALING (145) 10-73
SIGNALING (146) 10-73
SIGNALING (147) 10-74
SIGNALING (148) 10-74
SIGNALING (150) 10-75
SIGNALING (151) 10-75
SIGNALING (152) 10-76
SIGNALING (166) 10-76
SIGNALING (167) 10-77

Monitoring Signaling Events 10-78

Test Report - Signaling (1) 10-82
Invalid Message Received - Signaling (4) 10-82
Database Module Function Call Failure - Signaling (6) 10-82
Socket Failure - Signaling (7) 10-83
Session Initiation Protocol Message Receive Failure - Signaling (8) 10-83
Timeout on Internet Protocol Address - Signaling (9) 10-83
Failed to Send Complete Session Initiation Protocol Message - Signaling (10) 10-83
Failed to Allocate Session Initiation Protocol Control Block - Signaling (11) 10-83
Feature Server is not Up or is not Responding to Call Agent - Signaling (12) 10-83
Signaling System 7 Signaling Link Down - Signaling (13) 10-83
Link is Remotely Inhibited - Signaling (14) 10-84
Link is Locally Inhibited - Signaling (15) 10-84

Link is Congested - Signaling (16) **10-84**
Link: Local Processor Outage - Signaling (17) **10-84**
Link: Remote Processor Outage - Signaling (18) **10-84**
Link Set Inaccessible - Signaling (19) **10-84**
Link Set Congestion - Signaling (20) **10-84**
Route Set Failure - Signaling (21) **10-85**
Route Set Congested - Signaling (22) **10-85**
Destination Point Code Unavailable - Signaling (23) **10-85**
Destination Point Code Congested - Signaling (24) **10-85**
Unanswered Blocking - Signaling (25) **10-85**
Unanswered Unblocking Message - Signaling (26) **10-85**
Unanswered Circuit Group Blocking - Signaling (27) **10-86**
Unanswered Circuit Group Unblocking - Signaling (28) **10-86**
Unanswered Circuit Query Message - Signaling (29) **10-86**
Unanswered Circuit Validation Test - Signaling (30) **10-86**
Unanswered Reset Circuit - Signaling (31) **10-86**
Unanswered Group Reset - Signaling (32) **10-87**
Unanswered Release - Signaling (33) **10-87**
Unanswered Continuity Check Request - Signaling (34) **10-87**
Trunk Locally Blocked - Signaling (36) **10-87**
Trunk Remotely Blocked - Signaling (40) **10-87**
Continuity Testing Message Received on the Specified Circuit Identification Code - Signaling (42) **10-88**
Release Complete Received in Response to Reset Circuit Message on the Specified Circuit Identification Code - Signaling (43) **10-88**
Continuity Recheck is Performed on Specified Circuit Identification Code - Signaling (44) **10-88**
Circuit is UNEQUIPPED on Remote Side - Signaling (45) **10-88**
Specified Circuit Identification Code is Invalid for the Operation - Signaling (46) **10-88**
A General Processing Error Encountered - Signaling (49) **10-88**
Unexpected Message for the Call State is Received: Clear Call - Signaling (50) **10-89**
Set Trunk State as Remotely Unequipped - Signaling (51) **10-89**
Set Trunk State as NOT Remotely Blocked - Signaling (52) **10-89**
Set Trunk State as Remotely Blocked - Signaling (53) **10-89**
Circuit Validation Test Aborted - Signaling (54) **10-89**
Circuit Validation Successful - Signaling (55) **10-89**
Continuity Recheck Failed - Signaling (57) **10-90**
Continuity Recheck Successful - Signaling (58) **10-90**
Auto State Change for Integrated Services Digital Network Trunk Group by Media Gateway - Signaling (59) **10-90**
Integrated Services Digital Network STATUS Message Containing Error Indication Received - Signaling (60) **10-90**

Trunk Operational State Changed by Service Message - Signaling (61) **10-90**
Received Integrated Services Digital Network RESTART Message - Signaling (62) **10-91**
Media Gateway/Termination Faulty - Signaling (63) **10-91**
Media Gateway Adapter Running out of Shared Memory Pools - Signaling (64) **10-91**
Media Gateway Adapter Running out of Heap Memory - Signaling (65) **10-91**
Call Agent Internal Error (Because of Which Media Gateway Adapter has to Start Automatically) - Signaling (66) **10-91**
Media Gateway Endpoints are out of Service at Gateway - Signaling (68) **10-92**
Call Agent and Feature Server Communication Message Timeout - Signaling (69) **10-92**
Integrated Services Digital Network Unable to Restore D-channel Due to Failed Communication - Signaling (70) **10-92**
Integrated Services Digital Network Unable to Establish D-channel - Signaling (71) **10-92**
Integrated Services Digital Network - Calls Lost Due to D-channel Down for Period of Time - Signaling (72) **10-92**
Integrated Services Digital Network - Unable to Send RESTART Due to RESTART Timer Expired - Signaling (73) **10-93**
Integrated Services Digital Network: Unable to Send the SERVICE Due to the SERVICE Timer Expired - Signaling (74) **10-93**
Signaling System 7 Stack not Ready - Signaling (75) **10-93**
Timeout on Remote Instance - Signaling (76) **10-93**
Integrated Services Digital Network D-channel Switchover for Non-Facility Associated Signaling - Signaling (77) **10-93**
Integrated Services Digital Network Single D-channel Down for Non-Facility Associated Signaling - Signaling (78) **10-94**
Media Gateway Unreachable - Signaling (79) **10-94**
Out of Bounds, Memory/Socket Error - Signaling (80) **10-94**
Insufficient Heap Memory - Signaling (81) (H.323) **10-94**
Insufficient Shared Memory Pools - Signaling (82) (H.323) **10-94**
Error While Binding to Socket - Signaling (83) **10-94**
Reached Maximum Socket Limit - Signaling (84) (H.323) **10-95**
Initialization Failure - Signaling (85) **10-95**
Remote H323 Gateway is not Reachable - Signaling (86) (H.323) **10-95**
H323 Message Parsing Error - Signaling (87) (H.323) **10-95**
H323 Message Encoding Error - Signaling (88) (H.323) **10-95**
Gatekeeper not Available/Reachable - Signaling (89) **10-95**
Alternate Gatekeeper is not Responding - Signaling (90) **10-95**
Endpoint Security Violation - Signaling (91) (H.323) **10-96**
Invalid Call Identifier - Signaling (92) **10-96**
Invalid Call Reference Value - Signaling (93) **10-96**
Invalid Conference Identifier - Signaling (94) **10-96**
Invalid Message from the Network - Signaling (95) **10-96**

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

Number of Open Session Initiation Protocol Connections is Reaching Engineered Limit - Signaling (138) **10-103**
Signaling System 7 Trunk was Found to be in Erroneous State - Signaling (139) (SS7) **10-104**
Unanswered Information Message - Signaling (140) **10-104**
Address not Resolved by Domain Name System Server - Signaling (141) **10-104**
Session Initiation Protocol Trunk Operationally Out-of-Service - Signaling (142) **10-104**
Internet Protocol Interface Link to the Signaling System 7 Signaling Gateway is Down - Signaling (143) **10-104**
All Internet Interface Links to Signaling System 7 Signaling Gateway are Down - Signaling (144) **10-105**
One Internet Protocol Interface to Signaling System 7 Signaling Gateway is Down - Signaling (145) **10-105**
All Retransmission Attempts of Session Initiation Protocol Request or Response Failed - Signaling (146) **10-105**
Domain Name System Service Addresses Exhausted - Signaling (147) **10-105**
Softswitch Audit Released Stale Memory - Signaling (148) **10-106**
Stream Control Transmission Protocol Association Congested - Signaling (150) **10-106**
Termination Permanent Error Code Received - Signaling (151) **10-106**
Termination Transient Error Received - Signaling (152) **10-106**
No Routing Keys are Active - Signal (166) **10-106**
No Signaling Gateways are Active – Signaling (167) **10-107**
Troubleshooting Signaling Alarms **10-108**
Socket Failure - Signaling (7) **10-111**
Media Gateway Control Protocol **10-111**
Session Initiation Protocol **10-111**
Session Initiation Protocol Message Receive Failure - Signaling (8) **10-111**
Session Initiation Protocol **10-111**
Timeout on Internet Protocol Address - Signaling (9) **10-112**
Media Gateway Control Protocol **10-112**
Session Initiation Protocol **10-112**
Failed to Send Complete Session Initiation Protocol Message - Signaling (10) **10-112**
Failed to Allocate Session Initiation Protocol Control Block - Signaling (11) **10-112**
Feature Server is not Up or is not Responding to Call Agent - Signaling (12) **10-113**
Signaling System 7 Signaling Link Down - Signaling (13) **10-114**
Signal System 7 and Call Agent Fail-over Interaction **10-114**
Link is Remotely Inhibited - Signaling (14) **10-115**
Link is Locally Inhibited - Signaling (15) **10-115**
Link is Congested - Signaling (16) **10-115**
Link: Local Processor Outage - Signaling (17) **10-115**
Link: Remote Processor Outage - Signaling (18) **10-115**
Link Set Inaccessible - Signaling (19) **10-115**

Link Set Congestion - Signaling (20) **10-116**
Route Set Failure - Signaling (21) **10-116**
Route Set Congested - Signaling (22) **10-116**
Destination Point Code Unavailable - Signaling (23) **10-117**
Destination Point Code Congested - Signaling (24) **10-118**
Trunk Locally Blocked - Signaling (36) **10-118**
Trunk Remotely Blocked - Signaling (40) **10-118**
Auto State Change for Integrated Services Digital Network Trunk Group by Media Gateway - Signaling (59) **10-118**
Media Gateway/Termination Faulty - Signaling (63) **10-119**
Media Gateway Adapter Running out of Shared Memory Pools - Signaling (64) **10-119**
Media Gateway Adapter Running out of Heap Memory - Signaling (65) **10-119**
Call Agent Internal Error (Because of Which Media Gateway Adapter has to Start Automatically) - Signaling (66) **10-119**
Media Gateway Endpoints are out of Service at Gateway - Signaling (68) **10-119**
Call Agent and Feature Server Communication Message Timeout - Signaling (69) **10-120**
Signaling System 7 Stack not Ready - Signaling (75) **10-120**
Integrated Services Digital Network Single D-channel Down for Non-Facility Associated Signaling - Signaling (78) **10-120**
Media Gateway Unreachable - Signaling (79) **10-120**
Out of Bounds, Memory/Socket Error - Signaling (80) **10-120**
Insufficient Heap Memory - Signaling (81) (H.323) **10-121**
Insufficient Shared Memory Pools - Signaling (82) (H.323) **10-121**
Error While Binding to Socket - Signaling (83) **10-121**
Reached Maximum Socket Limit - Signaling (84) (H.323) **10-121**
Initialization Failure - Signaling (85) **10-121**
Remote H323 Gateway is not Reachable - Signaling (86) (H.323) **10-121**
H323 Message Parsing Error - Signaling (87) (H.323) **10-122**
H323 Message Encoding Error - Signaling (88) (H.323) **10-122**
Gatekeeper not Available/Reachable - Signaling (89) **10-122**
Alternate Gatekeeper is not Responding - Signaling (90) **10-122**
Endpoint Security Violation - Signaling (91) (H.323) **10-123**
Invalid Call Identifier - Signaling (92) **10-123**
Invalid Call Reference Value - Signaling (93) **10-123**
Invalid Conference Identifier - Signaling (94) **10-123**
Invalid Message from the Network - Signaling (95) **10-123**
Internal Call Processing Error - Signaling (96) **10-124**
Insufficient Information to Complete Call - Signaling (97) **10-124**
H323 Protocol Inconsistencies - Signaling (98) (H.323) **10-124**
Abnormal Call Clearing - Signaling (99) **10-124**

Codec Negotiation Failed - Signaling (100) **10-124**
Per Call Security Violation - Signaling (101) **10-124**
H323 Network Congested - Signaling (102) (H.323) **10-125**
Aggregation Connection Down - Signaling (103) **10-125**
Enhanced Subscriber Authentication Cisco BTS 10200 Softswitch Delivery Function Connection Down - Signaling (106) **10-125**
Logical Internet Protocol Addresses not Mapped Correctly - Signaling (107) **10-125**
Simplex Only Operational Mode - Signaling (108) **10-126**
Stream Control Transmission Protocol Association Failure - Signaling (109) **10-126**
Message Transfer Part 3 User Adapter Troubleshooting Procedure **10-126**
Signaling Connection Control Part User Adapter Troubleshooting Procedures **10-129**
Signaling Gateway Group Is Out-of-Service - Signaling (110) **10-130**
Stream Control Transmission Protocol Association Degraded (One of Two Internet Protocol Connections Down) - Signaling (111) **10-130**
Message Transfer Part 3 User Adapter Troubleshooting Procedure **10-130**
Signaling Connection Control Part User Adapter Troubleshooting Procedure **10-130**
Stream Control Transmission Protocol Association Configuration Error - Signaling (112) **10-130**
Message Transfer Part 3 User Adapter Troubleshooting Procedure **10-131**
Signaling Connection Control Part User Adapter Troubleshooting Procedure **10-131**
Signaling Gateway Failure - Signaling (113) **10-131**
Signaling Gateway Process Is Out-of-Service - Signaling (114) **10-131**
Destination Point Code User Part Unavailable - Signaling (116) **10-132**
Circuit Validation Test Message Received for an Unequipped Circuit Identification Code - Signaling (117) **10-132**
Circuit Verification Response Received with Failed Indication - Signaling (118) **10-132**
Signaling System 7 Adapter Process Faulty - Signaling (119) **10-132**
Signaling System 7 Module/Signaling System 7 Adapter Faulty - Signaling (120) **10-132**
Message Transfer Part 3 User Adapter Cannot Go Standby - Signaling (121) **10-133**
Message Transfer Part 3 User Adapter Cannot Go Active - Signaling (122) **10-133**
Remote Subsystem is Out Of Service - Signaling (124) **10-133**
Signaling Connection Control Part Routing Error - Signaling (125) **10-133**
Signaling Connection Control Part Binding Failure - Signaling (126) **10-134**
Transaction Capabilities Application Part Binding Failure - Signaling (127) **10-134**
Session Initiation Protocol Trunk Operationally Out-of-Service - Signaling (142) **10-134**
Internet Protocol Interface Link to the Signaling System 7 Signaling Gateway is Down - Signaling (143) **10-134**
All Internet Protocol Interface Links to Signaling System 7 Signaling Gateway are Down - Signaling (144) **10-134**
One Internet Protocol Interface to Signaling System 7 Signaling Gateway is Down - Signaling (145) **10-135**
Stream Control Transmission Protocol Association Congested - Signaling (150) **10-135**

Termination Permanent Error Code Received - Signaling (151) 10-135

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
SYSTEM (13) 12-9
SYSTEM (14) 12-9
SYSTEM (15) 12-10

Monitoring System Events 12-11

Test Report - System (1) 12-11
Inter-Process Communication Queue Read Failure - System (2) 12-11
Inter-Process Communication Message Allocate Failure - System (3) 12-11
Inter-Process Communication Message Send Failure - System (4) 12-12
Unexpected Inter-Process Communication Message Received - System (5) 12-12
Index List Insert Error - System (6) 12-12
Index List Remove Error - System (7) 12-12
Thread Creation Failure - System (8) 12-12
Timer Start Failure - System (9) 12-12
Index Update Registration Error - System (10) 12-13
Index Table Add-Entry Error - System (11) 12-13
Software Error - System (12) 12-13
Multiple Readers and Multiple Writers Maximum Q Depth Reached - System (13) 12-13
Multiple Readers and Multiple Writers Queue Reached Low Queue Depth - System (14) 12-13
Multiple Readers and Multiple Writers Throttle Queue Depth Reached - System (15) 12-13

Troubleshooting System Alarms 12-14

Inter-Process Communication Queue Read Failure - System (2) 12-14
Inter-Process Communication Message Allocate Failure - System (3) 12-14
Inter-Process Communication Message Send Failure - System (4) 12-15
Index List Insert Error - System (6) 12-15

Index List Remove Error - System (7) 12-15
Thread Creation Failure - System (8) 12-15
Index Update Registration Error - System (10) 12-15
Index Table Add Entry Error - System (11) 12-16
Software Error - System (12) 12-16
Multiple Readers and Multiple Writers Maximum Q Depth Reached - System (13) 12-16
Multiple Readers and Multiple Writers Queue Reached Low Queue Depth - System (14) 12-16
Multiple Readers and Multiple Writers Throttle Queue Depth Reached - System (15) 12-16

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 13-7
Oracle Database Tool Restart 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 14-7
Trunk Reason Responses 14-9
Trunk Termination Reason Responses, Signaling System 7 Only 14-10
Fault Reason Responses 14-11
Protocol Troubleshooting 14-12
Troubleshooting Signaling System 7 SIGTRAN Problems 14-12
Cisco Internet Protocol Transfer Point Troubleshooting Procedures 14-12

Using Cisco BTS 10200 Softswitch Command Line Interface Commands 14-14
Viewing Cisco BTS 10200 Softswitch Logs 14-14
'Troubleshooting Transaction Capabilities Application Part with the Query Verification Tool 14-15
Debugging Network Related Transaction Capabilities Application Part/Signaling Connection Control Part Problems 14-16
Troubleshooting H.323 Problems 14-22
Outgoing Trunk Group is Out of Service 14-22
Outgoing H.323 Gateway is Out of Service 14-23
H.323 Gateway Fails to Register With Gatekeeper (Invalid Alias) 14-24
Outgoing H.323 Gateway Unregistered With Gatekeeper and Needs to Use Registration, Admissions, and Status 14-25
Stable Calls Are Dropped When Call Agent Switches Over 14-26
No Matching Dial Plan Found on Incoming H.323 Trunk Group 14-26
Configuration at Softswitch or Gatekeeper Has Placed Routing Into a Loop 14-27
Outgoing H.323 Calls Routed to Incorrect Endpoint When Using Registration, Admissions, and Status 14-27
Outgoing H.323 Calls Routed to Incorrect Endpoint When Using Direct Signaling 14-28
Registration, Admissions, and Status Still Used When Outgoing H.323 Call is Provisioned to Use Direct Signaling 14-29
Troubleshooting Integrated Services Digital Network Problems 14-30
How to Troubleshoot When the Integrated Services Digital Network Trunk Group Fails to Restore 14-30
Checking the Status of a Trunk Termination 14-32
Checking Media Gateway Provisioning 14-34
Additional Command Line Interface Verification 14-37
Maintenance of a Call Agent Connected to an Integrated Services Digital Network Trunk Group 14-38
File Configuration – bts.properties 14-38
File Extraction and Editing – bts.properties 14-39
Privacy Screening Troubleshooting 14-39
Symptom One 14-39
Solution One 14-39
Symptom Two 14-40
Solution Two 14-40
Symptom Three 14-40
Solution Three 14-40
Symptom Four 14-40
Solution Four 14-40

CHAPTER 15 **Diagnostic Tests** 15-1

Introduction 15-1

Media Gateway Tests 15-2

Subscriber Termination Tests 15-3

Signaling System 7 Trunk Termination Tests 15-5

Integrated Services Digital Network Trunk Termination Tests 15-8

Channel-Associated Signaling Trunk Termination Tests 15-9

Announcement Trunk Termination Tests 15-11

Troubleshooting Using Snoop 15-12

Query Verification Tool and Translation Verification Tool 15-16

Tool Requirements 15-16

Query Verification Tool 15-16

Overview 15-17

Command Format 15-17

Response Format 15-18

Query Errors 15-19

Query Verification Tool Measurements 15-22

Translation Verification Tool 15-22

Overview 15-23

Command Format 15-23

Response Format 15-23

Translation Verification Tool Measurements 15-24

Using Query Verification Tool and Translation Verification Tool Together 15-25

LNP Examples 15-26

Example 1 15-26

Example 2 15-28

Example 3 15-30

Example 4 15-31

Example 5 15-33

Network Loopback Test for Network-based Call Signaling/Media Gateway Control Protocol Endpoints 15-34

Overview 15-34

Restrictions 15-35

Installing 15-35

Configuring 15-35

Configuration Examples 15-35

Using/Operating the Network Loopback Test for Network-based Call Signaling/Media Gateway Control Protocol Endpoints 15-39

Dedicated Test Trunk Group 15-40

Shared Test Trunk Group 15-40
Configuring the Originating Trunk Group 15-41
Session Initiation Protocol Subscriber Registration Status Check 15-41
System Health Report 15-42
Fast Audit and Sync Tool 15-42
Restrictions and Limitations 15-43
Using the bts_audit Tool 15-43
Using the bts_sync Tool 15-43
Command Parameters 15-43
Command Responses 15-44
Database Out of Synchronization 15-44
ISDN Network Loopback Test 15-44
Configuring 15-45
Originating Trunk Group 15-45
Call Agent Configuration Table 15-45
Dial Plan 15-46
Sample Configurations 15-46
Line Loopback Tests over an ISDN Trunks 15-46
Trunk Loopback Tests over an ISDN Trunk 15-52
Enhanced Traffic Measurement 15-53
Measurement Data Transport and Access 15-54
Measurement Data Event Reports 15-54
Operating 15-55
Provisioning Measurement Report Types 15-55
Measurement Report Summaries 15-57
Reporting Current Interval Counts 15-61
Clearing Current Interval Counts 15-64
Measurements 15-67
ISDN Protocol Counters 15-67
Call Processing Counters 15-69
MGCP Adapter Counters 15-76
Session Initiation Protocol Counters 15-77
PSTN Trunk Testing 15-80
Test Overview 15-80
Cisco BTS 10200 Originating Test Line 15-81
Function 15-81
Test Equipment 15-81
Test Line 15-81
Trunk Access 15-81

Trunk Access and Test Termination Number Format 15-82
Trunk Under Test Outpulsing 15-82
Cisco BTS 10200 Terminating Test Line 15-83
Function 15-83
Test Equipment 15-83
Test Line 15-83
TTL Dial Plan 15-83
Near End Test Origination Test Line 15-84
Far End Originating Test Line 15-85
Function 15-85
Test Equipment 15-85
Test Line 15-85
Trunk Access 15-85
Trunk Access and Test Termination Number Format 15-85
Trunk Under Test Outpulsing 15-85
Far End Terminating Test Line 15-86
Function 15-86
Test Equipment 15-86
Test Line 15-86
TTL Dial Plan 15-86
1xx Test Lines 15-87
1xx Test Line Support 15-87
100 Test–Balance 15-88
101 Test–Communications and Test 15-88
102 Test–Milliwatt 15-88
103 Test–Signaling and Supervisory 15-88
104 Test–2-Way Test 15-88
105 Test–ROTL/Responder 15-88
107 Test Line–Data Transmission 15-89
108 Test–Digital Loopback 15-89
109 Test–Echo 15-89

CHAPTER 16 **Disaster Recovery Procedures** 16-1
Introduction 16-1
Restarting a Cisco BTS 10200 Softswitch Process 16-1
Disaster Recovery From Flash Archive 16-1
Before You Begin 16-2
Flash Archive Restore 16-2
Setting up Interfaces 16-4

Restoring the Cisco BTS 10200 Softswitch Application 16-5
Power Failure Recovery 16-6
Power Fail Occurs Procedure 16-6
Power is Restored Procedure 16-6
Power Failure Scenarios 16-7
Power Failure on Single Host Computer 16-7
Recovery Procedure 16-7
Power Failure on Both Call Agent Computers 16-8
Power Failure on Both Element Management System Computers 16-9
Total System Power Outage 16-9
Element Management System Database Recovery from Hot Backup 16-10
Recovery Goal 16-10
Recovering the Primary Element Management System Database 16-11
Post Recovery – Cold Backup 16-14
Recovering the Element Management System Database from Another Database 16-15
Recovery Procedures 16-15
Fresh Download 16-23
Call Agent Database Download and Recovery 16-24
Recovering Shared Memory Data 16-26
Recovering Shared Memory 16-26
Restoring Subscriber and Trunk Terminations to Service 16-28
Controlling Trunks and Trunk Groups 16-29
Using the cs-control Tool to Bring Subscribers In-Service 16-29
Disaster Recovery Using the Automatic Shared Memory Backup 16-29
Before You Begin 16-30
Automatic Shared Memory Backup Restore 16-30
Restore Shared Memory Script 16-31

CHAPTER 17 **Disk Replacement** 17-1
Introduction 17-1
Full System Backup Procedure 17-2
Call Agent/Feature Server Backup 17-2
Element Management System/Bulk Data Management System Backup 17-4
Call Agent/Feature Server or Element Management System Disk 0 Replacement 17-5
Call Agent/Feature Server or Element Management System Disk 1 Replacement 17-9

APPENDIX A **Recoverable and Nonrecoverable Error Codes** A-1

APPENDIX B **System Usage of MGW Keepalive Parameters, Release 4.5.x** B-1

Provisionable Parameters B-1

Definitions and Additional Parameters B-3

Examples of Successful MGCP Message Transmissions B-4

Initial Transmission Waiting Period (mgcp-t-tran) B-4

Scenarios with AUEP Message Retransmissions and ACK Received B-4

Scenarios with AUEP Message Retransmissions and No ACK B-6

MGCP-RTO-MAX B-6

MGCP-MAX2-RETRIES and MGCP-T-MAX B-6

Keepalive Process B-7

Scenario 1—MGW Reachable B-7

Basic Scenario B-8

MGCP Message Sent and Is Unsuccessful B-9

MGCP Message Sent and Is Successful B-10

Scenario 2 (Special Case)—Reachable RGW with 16 or Fewer Endpoints and No Stable Calls In Progress B-10

Basic Scenario B-11

MGCP Message Sent and Is Unsuccessful B-12

MGCP Message Sent and Is Successful B-13

Scenario 3—MGW Unreachable B-13

KA Attempts Unsuccessful, MGW Unreachable, and Stable Call Is Present B-13

KA Attempts Unsuccessful, MGW Unreachable, and No Stable Calls Present B-15

MGW Unreachable, New Call Termination Attempt Occurs B-16

GLOSSARY

Preface

Revised: July 22, 2009, OL-8000-32

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, "Recoverable and Nonrecoverable Error Codes" – Lists normal, recoverable and nonrecoverable error codes for the Cisco BTS 10200 Softswitch.
- Appendix B, "System Usage of MGW Keepalive Parameters, Release 4.5.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 4.5.x

This document includes all of the information that was contained in the previous issue (the Release 4.5 Cisco BTS 10200 Softswitch Troubleshooting Guide, OL-8000-08), and has been updated for the Release 4.5 Cisco BTS 10200 Softswitch Troubleshooting Guide, OL-8000-09 as described in this Preface.

Updates are contained in the following chapters and appendixes of this document:

- Updated Chapter 16, “Disaster Recovery Procedures”

Additionally, this document has been updated to OL-8000-10. Updates are contained in the following chapters and sections:

- Updated Chapter 6, “Database Troubleshooting”
- Updated Chapter 6, “DATABASE (11)”
- Updated Chapter 6, “Element Management System Database Alert.log Alerts - Database (11)”

The updates to this document to OL-8000-11 include:

- Removed AUDIT (9) event information
- Added BILLING (60), MAINTENANCE (119), MAINTENANCE (120), SIGNALING (166), SIGNALING (167), and SYSTEM (15) event information.

The updates to this document for OL-8000-12 include:

- Adding Appendix B, “System Usage of MGW Keepalive Parameters, Release 4.5.x” to the document.

The updates to this document for OL-8000-13 include:

- Updated Chapter 16, “Disaster Recovery Procedures” to include the procedure for restoration of the Automatic Shared Memory Backup (ASMB)

The updates to this document for OL-8000-14 include:

- Updated Chapter 16, “Disaster Recovery Procedures”

The updates to this document for OL-8000-15 included:

- Updated DATABASE (11) primary cause and primary action

The updates to this document for OL-8000-16 included:

- Updated Chapters 14, 15, and 16 to include troubleshooting information for Release 4.5.1.

The updates to this document for OL-8000-17 included:

- Updated Chapter 7 to include the Maintenance 122 and Maintenance 123 alarms and events.

The update to this document for OL-8000-18 included:

- Removal of the Release Cause Code appendix, update of Chapter 14 and Chapter 15, and update of the System Usage of MGW Keepalive Parameters appendix.

The update of this document for OL-8000-19 included:

- Update of the threshold and throttle information in Chapter 1

The updates of this document for OL-8000-20 and OL-8000-21 included:

- Update of the keepalive information in Appendix B.

The update of this document from OL-8000-21 to OL-8000-22 include incorporating the delta alarm and event information from Release 3.5 to Release 4.5.x.

The update of this document from OL-8000-22 to OL-8000-23 included:

- Update of the keepalive information in Appendix B.

The update of this document from OL-8000-23 to OL-8000-24 included:

- Adding the event and alarm differences between release 4.5.13 and 4.5.1.

The update of this document from OL-8000-24 to OL-8000-25 included:

- Removing the Throttle/Threshold erroneous note

The update of this document from OL-8000-25 to OL-8000-26 included updating the disk replacement procedures in Chapter 17.

The update of this document from OL-8000-26 to OL-8000-27 included updating the recovering shared memory procedure and call agent database download and restore.

The update to OL-8000-28 included updating the information for the Audit 4 alarm.

The update to OL-8000-29 included adding the "PSTN Trunk Testing" section on page 15-80 to Chapter 15.

The update to OL-8000-30 included making changes to the "Automatic Shared Memory Backup Restore" section on page 16-30.

The update to OL-8000-31 included adding the "Oracle Database Tool Restart" section on page 13-8.

The update to OL-8000-32 included updating the "Recovering Shared Memory" section on page 16-26.

New Events and Alarms (Release 3.5 to Release 4.5.1)

Table 1 lists the new events and alarms that were incorporated into the BTS 10200 system as part of the update from Release 3.5 to Release 4.5.1.

Table 1 New Events and Alarms (Release 3.5 to Release 4.5.1)

Type and Number	Description
AUDIT (2)	Start or Stop of Signaling System 7-Circuit Identification Code Audit
AUDIT (3)	Signaling System 7 Circuit Identification Code Audit Terminated Before Successful Completion
AUDIT (4)	Call Exceeds a Long-Duration Threshold
AUDIT (6)	Major Internal Audit Failure
AUDIT (7)	Minor Internal Audit Failure
AUDIT (8)	Warning From Internal Audit
AUDIT (10)	Call Data Audit Complete
AUDIT (11)	Critical Network Time Protocol Service Failure
AUDIT (12)	Major Network Time Protocol Service Failure
AUDIT (13)	Minor Network Time Protocol Service Failure
AUDIT (14)	Network Time Protocol Service Warning
AUDIT (15)	Critical Index Shared Memory Error
AUDIT (16)	Process Heap Memory Usage Exceeds Minor Threshold Level
AUDIT (17)	Process Heap Memory Usage Exceeds Major Threshold Level
AUDIT (18)	Process Heap Memory Usage Exceeds Critical Threshold Level
AUDIT (19)	Recovered Memory of Stale Call
AUDIT (20)	Audit Found Lost Call Data Record
BILLING (52)	Bulk Data Management System Stopped Generating New Billing File
BILLING (57)	Prepaid Subscriber Call Attempt Failed Because of Balance
BILLING (58)	Signaling Prepaid Server Inaccessible
BILLING (60)	Bad File Detected During Startup
CALLP (38)	Release Cause 25 Exchange Routing Error Received
CALLP (39)	Test Call Blocked Due to Congestion or Isolation
CALLP (40)	Interactive Voice Response Real Time Transport Protocol Session Fail
CALLP (41)	INVITE Message From Unauthorized Call Agent
CONFIG (5)	Feature-Server Database and Command Line Host Mismatch
DATABASE (19)	Daily Database Backup Completed Successfully
DATABASE (20)	Replication Data Flush Timeout During Switchover
DATABASE (21)	Database Statistics Collection Exception
DATABASE (25)	Secure File Transfer Protocol Transfer Failed
DATABASE (26)	File Write Error

Table 1 New Events and Alarms (Release 3.5 to Release 4.5.1) (continued)

Type and Number	Description
MAINTENANCE (86)	System Health Report Collection Error
MAINTENANCE (87)	Status Update Process Request Failed
MAINTENANCE (88)	Status Update Process Database List Retrieval Error
MAINTENANCE (89)	Status Update Process Database Update Error
MAINTENANCE (90)	Disk Partition Moderately Consumed
MAINTENANCE (91)	Internet Protocol Manager Configuration File Error
MAINTENANCE (92)	Internet Protocol Manager Initialization Error
MAINTENANCE (93)	Internet Protocol Manager Interface Failure
MAINTENANCE (94)	Internet Protocol Manager Interface State Change
MAINTENANCE (95)	Internet Protocol Manager Interface Created
MAINTENANCE (96)	Internet Protocol Manager Interface Removed
MAINTENANCE (102)	Thread Watchdog Counter Close to Expiry for a Thread
MAINTENANCE (103)	Central Processing Unit is Offline
MAINTENANCE (104)	Aggregration Device Address Successfully Resolved
MAINTENANCE (105)	Unprovisioned Aggregration Device Detected
MAINTENANCE (106)	Aggregration Device Address Resolution Failure
MAINTENANCE (107)	No Heartbeat Messages Received Through Interface From Router
MAINTENANCE (108)	A Log File Cannot be Transferred
MAINTENANCE (109)	Five Successive Log Files Cannot be Transferred
MAINTENANCE (110)	Access to Log Archive Facility Configuration File Failed or File Corrupted
MAINTENANCE (111)	Cannot Login to External Archive Server
MAINTENANCE (119)	Periodic Shared Memory Database Backup Failure
MAINTENANCE (120)	Periodic Shared Memory Database Backup Success
MAINTENANCE (122)	Northbound Provisioning Message is Retransmitted
MAINTENANCE (123)	Northbound Provisioning Message Dropped Due To Full Index Table
SECURITY (2)	Invalid Credentials Presented by a Session Initiation Protocol Phone
SECURITY (3)	Internet Protocol Security Connection Down
SECURITY (4)	Internet Protocol Security Media Terminal Adapter Key Establish Error
SECURITY (5)	Internet Protocol Security Outgoing Security Association Not Found
SECURITY (6)	Secure Session Initiation Protocol Endpoint Validation Failure
SIGNALING (109)	Stream Control Transmission Protocol Association Failure
SIGNALING (110)	Signaling Gateway Group is Out-of-Service
SIGNALING (111)	Stream Control Transmission Protocol Association Degraded (One of Two Internet Protocol Connections Down)
SIGNALING (112)	Stream Control Transmission Protocol Association Configuration Error
SIGNALING (113)	Signaling Gateway Failure

Table 1 New Events and Alarms (Release 3.5 to Release 4.5.1) (continued)

Type and Number	Description
SIGNALING (114)	Signaling Gateway Process is Out-of-Service
SIGNALING (115)	Invalid Routing Context Received
SIGNALING (116)	Destination Point Code User Part Unavailable
SIGNALING (121)	Message Transfer Part 3 User Adapter Cannot Go Standby
SIGNALING (122)	Message Transfer Part 3 User Adapter Cannot Go Active
SIGNALING (124)	Remote Subsystem is Out Of Service
SIGNALING (125)	Signaling Connection Control Part Routing Error
SIGNALING (126)	Signaling Connection Control Part Binding Failure
SIGNALING (127)	Transaction Capabilities Application Part Binding Failure
SIGNALING (132)	Transaction Capabilities Application Part Reaches the Provisioned Resource Limit
SIGNALING (133)	Unable to Decode Generic Transport Descriptor Message
SIGNALING (134)	Signaling System 7 Message Encoding Failure
SIGNALING (135)	Signaling System 7 Message Decoding Failure
SIGNALING (136)	Signaling System 7 Message Invalid Received
SIGNALING (137)	Signaling System 7 Confusion Message Received
SIGNALING (138)	Number of Open Session Initiation Protocol Connections is Reaching Engineered Limit
SIGNALING (139)	Signaling System 7 Trunk was Found to be in Erroneous State
SIGNALING (140)	Unanswered Information Message
SIGNALING (141)	Address not Resolved by Domain Name System Server
SIGNALING (142)	Session Initiation Protocol Trunk Operationally Out-of-Service
SIGNALING (143)	Internet Protocol Interface Link to the Signaling System 7 Signaling Gateway is Down
SIGNALING (144)	All Internet Protocol Interface Links to Signaling System 7 Signaling Gateway are Down
SIGNALING (145)	One Internet Protocol Interface to Signaling System 7 Signaling Gateway is Down
SIGNALING (146)	All Retransmission Attempts of Session Initiation Protocol Request or Response Failed
SIGNALING (147)	Domain Name System Service Addresses Exhausted
SIGNALING (150)	Stream Control Transmission Protocol Association Congested
SIGNALING (151)	Termination Permanent Error Code Received
SIGNALING (152)	Termination Transient Error Received
SIGNALING (166)	No Routing Keys are Active
SIGNALING (167)	No Signaling Gateways are Active
STATISTICS (12)	Measurement Handshake Error - Schema Inconsistency

Table 1 New Events and Alarms (Release 3.5 to Release 4.5.1) (continued)

Type and Number	Description
STATISTICS (13)	Traffic and Measurements Module Application Programming Interface Failure
SYSTEM (12)	Software Error
SYSTEM (13)	Multiple Readers and Multiple Writers Maximum Queue Depth Reached
SYSTEM (14)	Multiple Readers and Multiple Writers Queue Reached Low Queue Depth
SYSTEM (15)	Multiple Readers and Multiple Writers Throttle Queue Depth Reached

Modified Events and Alarms (Release 3.5 to Release 4.5.1)

Table 2 lists the BTS 10200 modified events and alarms that were modified as part of the upgrade from Release 3.5 to Release 4.5.1.

Table 2 Modified Events and Alarms (Release 3.5 to Release 4.5.1)

Type and Number	Description
BILLING (6)	File Transfer Protocol/Secure File Transfer Protocol Transfer Failed
BILLING (13)	Database Connection Error
BILLING (14)	File Open Error
BILLING (15)	File Write Error
BILLING (33)	File Transfer Protocol/Secure File Transfer Protocol Parameters Invalid
BILLING (41)	Message Content Error
BILLING (44)	Record Keeping System Switch Occurred
BILLING (45)	Event Message Log File Opened
BILLING (46)	Event Message Log File Closed
BILLING (53)	Event Message Disk Space 50 Percent Full
BILLING (56)	Billing Data Corruption Detected
CALLP (9)	No Route Available for Carrier Dialed
DATABASE (5)	Element Management System Database HeartBeat Process Died
DATABASE (17)	Data Replication Failed
MAINTENANCE (41)	Administrative State Change Successful with Warning
MAINTENANCE (47)	Thread Watchdog Counter Expired for a Thread
MAINTENANCE (57)	Memory and Swap are Consumed at Critical Levels
MAINTENANCE (58)	Memory and Swap are Consumed at Abnormal Levels
MAINTENANCE (65)	Disk Partition Critically Consumed
MAINTENANCE (66)	Disk Partition Significantly Consumed
MAINTENANCE (71)	Local Domain Name System Server Response Too Slow
MAINTENANCE (72)	External Domain Name System Server Response Too Slow
MAINTENANCE (73)	External Domain Name System Server not Responsive
MAINTENANCE (82)	Average Outgoing Heartbeat Period Exceeds Critical Limit
OSS (6)	Structured Query Language Connection Error
SIGNALING (23)	Destination Point Code Unavailable
SIGNALING (25)	Unanswered Blocking
SIGNALING (26)	Unanswered Unblocking Message
SIGNALING (27)	Unanswered Circuit Group Blocking
SIGNALING (28)	Unanswered Circuit Group Unblocking
SIGNALING (29)	Unanswered Circuit Query Message
SIGNALING (30)	Unanswered Circuit Validation Test

Table 2 Modified Events and Alarms (Release 3.5 to Release 4.5.1) (continued)

Type and Number	Description
SIGNALING (31)	Unanswered Reset Circuit
SIGNALING (32)	Unanswered Group Reset
SIGNALING (33)	Unanswered Release
SIGNALING (34)	Unanswered Continuity Check Request
SIGNALING (42)	Continuity Testing Message Received on the Specified Circuit Identification Code
SIGNALING (43)	Release Complete Received in Response to Reset Circuit Message on the Specified Circuit Identification Code
SIGNALING (44)	Continuity Recheck is Performed on Specified Circuit Identification Code
SIGNALING (45)	Circuit is UNEQUIPPED on Remote Side
SIGNALING (46)	Specified Circuit Identification Code is Invalid for the Operation
SIGNALING (49)	A General Processing Error Encountered
SIGNALING (50)	Unexpected Message for the Call State is Received: Clear Call
SIGNALING (51)	Set Trunk State as Remotely Unequipped
SIGNALING (52)	Set Trunk State as NOT Remotely Blocked
SIGNALING (53)	Set Trunk State as Remotely Blocked
SIGNALING (54)	Circuit Validation Test Aborted
SIGNALING (55)	Circuit Validation Successful
SIGNALING (57)	Continuity Recheck Failed
SIGNALING (58)	Continuity Recheck Successful
SIGNALING (68)	Media Gateway Endpoints are out of Service at Gateway
SIGNALING (69)	Call Agent and Feature Server Communication Message Timeout
SIGNALING (89)	Gatekeeper not Available/Reachable
SIGNALING (90)	Alternate Gatekeeper is not Responding
SIGNALING (107)	Logical Internet Protocol Addresses not Mapped Correctly
SIGNALING (108)	Simplex Only Operational Mode
SIGNALING (118)	Circuit Verification Response Received with Failed Indication

Deprecated Events and Alarms (Release 4.5 to Release 4.5.1)

Table 3 lists the BTS 10200 events and alarms that were deprecated as part of the upgrade from Release 3.5 to Release 4.5.1.

Table 3 Deprecated Events and Alarms (Release 3.5 to Release 4.5.1)

Type and Number	Description
BILLING(9)	Duplicate Event Message Received
BILLING (10)	Database Lock Error
BILLING (11)	Database Unlock Error
BILLING (12)	Table Pointer Read Error
BILLING(16)	Time Point Calculation Error
BILLING(17)	Shared Memory Add Failure
BILLING(18)	Error Calling MKTIME Function
BILLING(19)	Call Detail Block Database Write Error
BILLING(20)	Call Detail Block Database Read Error
BILLING(21)	Unknown Billing Event Message Received
BILLING(22)	Error Releasing Staging Area in Shared Memory
BILLING(23)	Error Releasing Busy List Entry in Shared Memory
BILLING(24)	Update Table Pointer Error
BILLING(26)	Shared Memory Update Failed
BILLING(27)	Shared Memory Entry Remove Failed
BILLING(28)	Wrong Port Number Specified
BILLING(34)	All Billing Links at CA Down
BILLING(39)	RADIUS Accounting Receive Failure
BILLING(43)	Invalid Billing Configuration—Program Exiting
MAINTENANCE(59)	Disk Reports Greater Than 70% Utilization
MAINTENANCE(60)	Disk Utilization has Returned to Normal Levels
SIGNALING(2)	Message Encoding Error
SIGNALING(3)	Message Decoding Error
SIGNALING(47)	Indicated Circuit is Out of Order
SIGNALING(48)	Indicated Circuit is Back in Service
SIGNALING(56)	Circuit Validation Failure
SIGNALING(67)	Gateway/Termination Returning Transient Error for the MGCP
SIGNALING(123)	Destination Point Code is Unavailable
SIGNALING(128)	INAP Binding Failure
SIGNALING(131)	INAP Reaches the Provisioned Resource Limit

New Events and Alarms (Release 4.5.13 to Release 4.5.1)

Table 4 lists the new events and alarms that were incorporated into the BTS 10200 system as part of the update from Release 4.5.13 to Release 4.5.1.

Table 4 New Events and Alarms (Release 4.5.13 to Release 4.5.1)

Type and Number	Description
BILLING (60)	Bad File Detected During Startup
DATABASE (25)	Secure File Transfer Protocol Transfer Failed
DATABASE (26)	File Write Error
MAINTENANCE (118)	Domain Name Server Zone Database does not Match Between the Primary Domain Name Server and the Internal Secondary Authoritative Domain Name Server (DNS Zone Database does not Match Between the Primary DNS and the ISADS)
MAINTENANCE (119)	Periodic Shared Memory Database Backup Failure
MAINTENANCE (120)	Periodic Shared Memory Database Backup Success
SYSTEM (9)	Timer Start Failure

Modified Events and Alarms (Release 4.5.13 to Release 4.5.1)

Table 5 lists the BTS 10200 modified events and alarms that were modified as part of the upgrade from Release 3.5 to Release 4.5.1.

Table 5 Modified Events and Alarms (Release 4.5.13 to Release 4.5.1)

Type and Number	Description
BILLING (6)	File Transfer Protocol/Secure File Transfer Protocol Transfer Failed
BILLING (14)	File Open Error
BILLING (15)	File Write Error
BILLING (56)	Billing Data Corruption Detected
SECURITY (6)	Secure Session Initiation Protocol Endpoint Validation Failure
SIGNALING (69)	Call Agent and Feature Server Communication Message Timeout
SIGNALING (148)	Softswitch Audit Released Stale Memory
SYSTEM (7)	Index List Remove Error

Deprecated Events and Alarms (Release 4.5.13 to Release 4.5.1)

There were no deprecated events or alarms between Release 4.5.13 and Release 4.5.1.

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS Version 2.0.

CHAPTER 1

Troubleshooting Overview

Revised: July 22, 2009, OL-8000-32

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

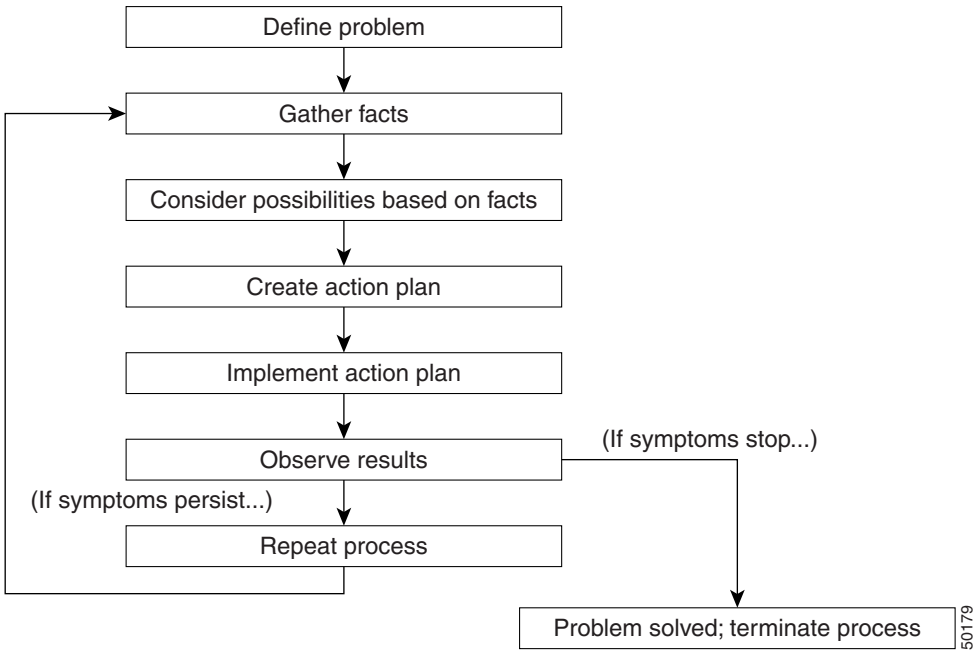
When you're troubleshooting in a telephony environment, a systematic approach always works best. An unsystematic approach to troubleshooting can result in a "quick fix." but it is usually a waste of valuable time and resources and often makes the situation worse.

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 Documentation and Submitting a Service Request" section on page liii 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 Documentation and Submitting a Service Request" section on page liii for detailed instructions on contacting Cisco TAC and opening a service request.

Figure 1-2 Problem Identification

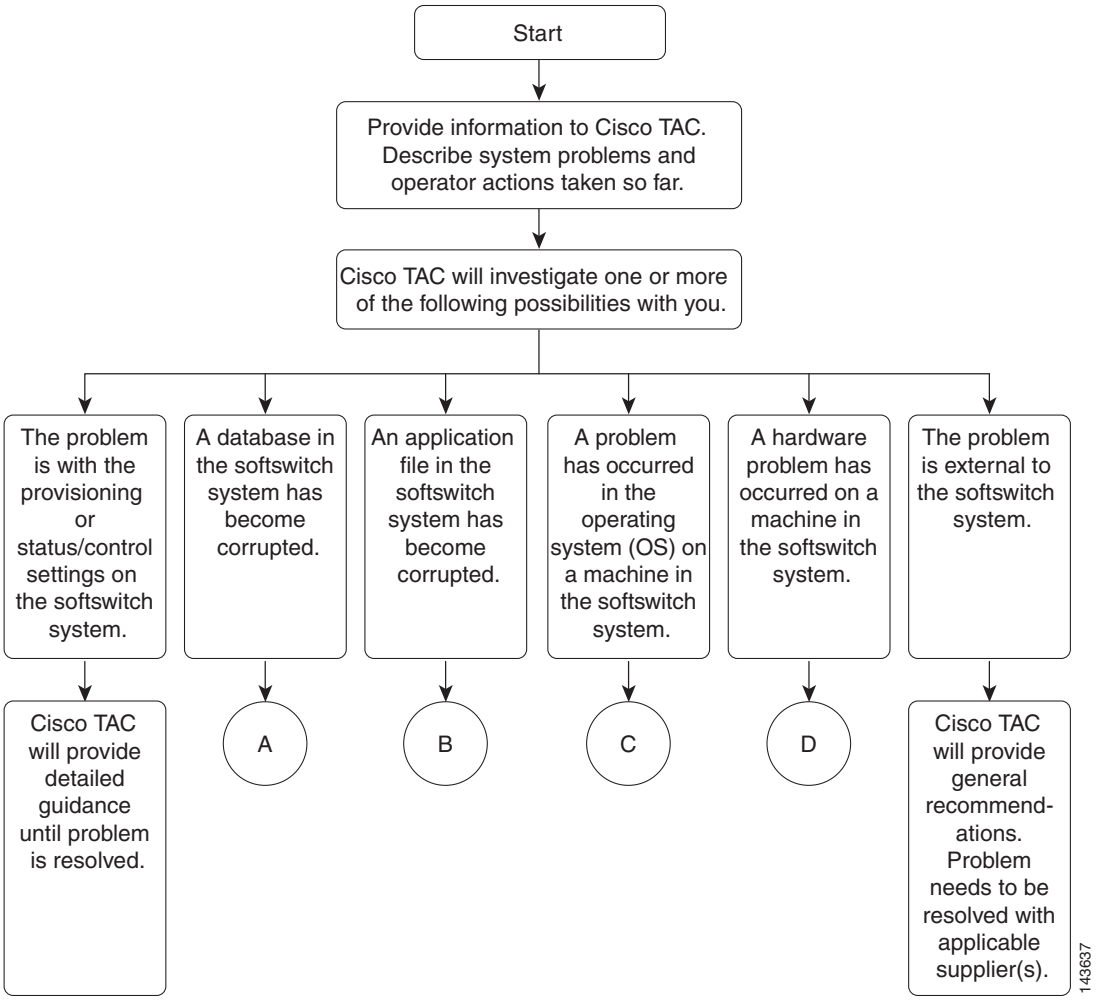
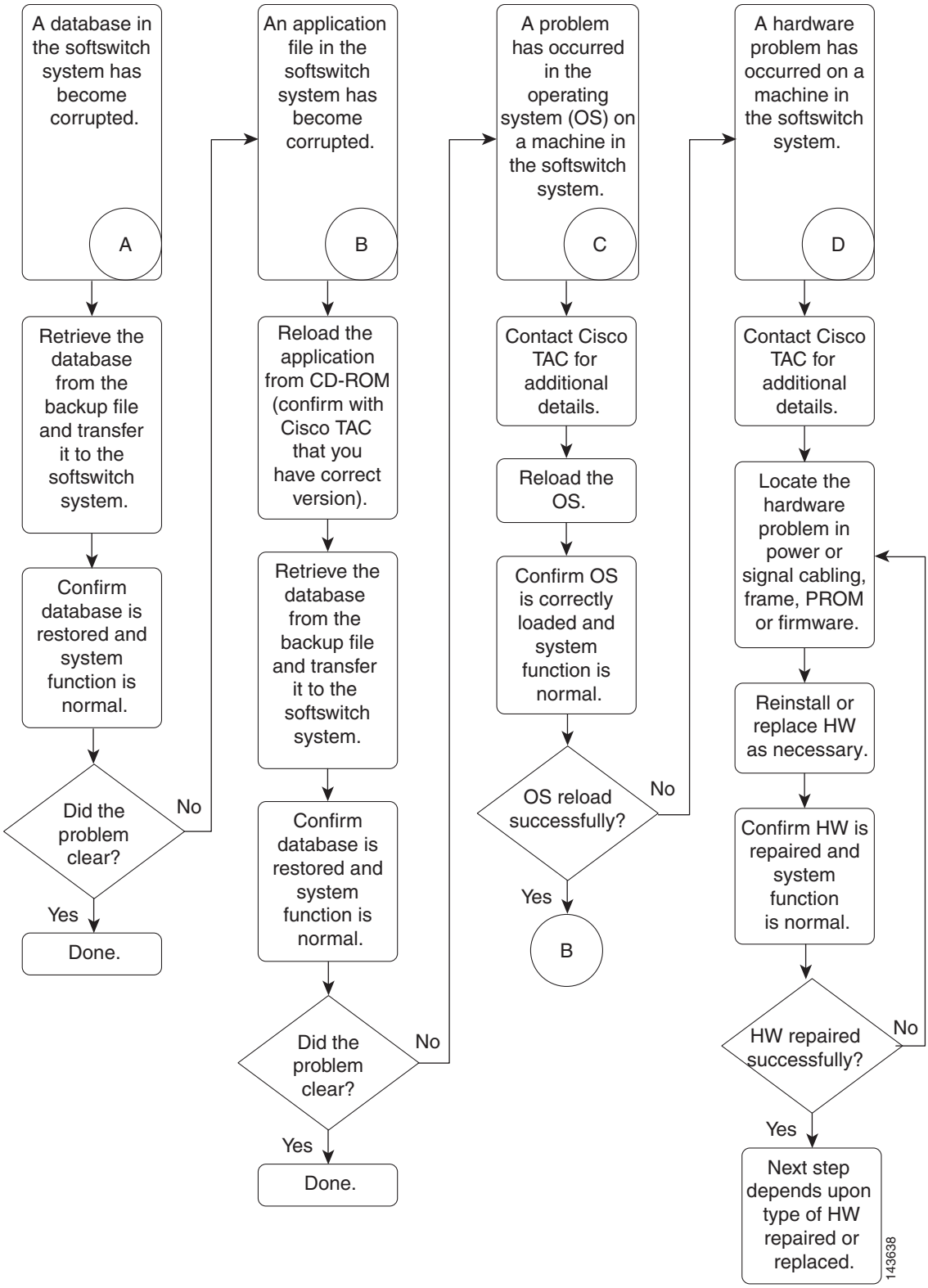


Figure 1-3 Resolving Database, Application, OS and Hardware Problems



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 1-17
  - 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=tg1@ca1.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=tg1@ca1.carrier.com
ORIGIN=bcm@ca146
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, `tg1@ca1.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 to12)
  - 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 1-17.

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.

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.

Throttle 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 and 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: July 22, 2009, OL-8000-32

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 (11)	AUDIT (12)	AUDIT (13)	AUDIT (4)	AUDIT (2)
AUDIT (18)	AUDIT (17)	AUDIT (16)	AUDIT (8)	AUDIT (10)
	AUDIT (20)		AUDIT (9)	AUDIT (14)
			AUDIT (15)	
			AUDIT (19)	

AUDIT (1)

For additional information, refer to the "Test Report - Audit (1)" section on page 2-12.

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 2-12.

DESCRIPTION	Start or Stop of Signaling System 7-Circuit Identification Code 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 2-13.

DESCRIPTION	Signaling System 7 Circuit Identification Code 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 2-13

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 2-17.

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 2-17.

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 2-17.

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 2-14.

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.

AUDIT (9)

To monitor and correct the cause of the event, refer to the "Softswitch Audit SIP CCB Release - Audit (9)" section on page 2-14.

DESCRIPTION	Softswitch Audit SIP CCB Release
SEVERITY	WARNING
THRESHOLD	100
THROTTLE	0
DATAWORDS	AORID - STRING [64] TGID - TWO_BYTES
PRIMARY CAUSE	One side of the BTS 10200 was inactive.
PRIMARY ACTION	The SIA determines that a network error or DNS error occurred.
SECONDARY CAUSE	A software error has occurred.
SECONDARY ACTION	Contact the BTS 10200 engineer. Contact Cisco TAC.

Refer to the "Obtaining Documentation and Submitting a Service Request" section on page liii for detailed instructions on contacting Cisco TAC and opening a service request.

AUDIT (10)

For additional information, refer to the "Memory Audit Complete Status - Audit (10)" section on page 2-14.

DESCRIPTION	Memory Audit Complete Status
SEVERITY	INFO
THRESHOLD	100
THROTTLE	0
DATAWORDS	Audit Type and Total Freed Count - STRING [256]
PRIMARY CAUSE	A SIP memory audit pass has been completed.
PRIMARY ACTION	Check to see if any call blocks are freed as a result of the audit. An investigation for root cause may be useful.

AUDIT (11)

To troubleshoot and correct the cause of the alarm, refer to the "Critical Network Time Protocol Service Failure - Audit (11)" section on page 2-18.

DESCRIPTION	Critical Network Time Protocol Service 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 (12)

To troubleshoot and correct the cause of the alarm, refer to the "Major Network Time Protocol Service Failure - Audit (12)" section on page 2-18.

DESCRIPTION	Major Network Time Protocol Service 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 (13)

To troubleshoot and correct the cause of the alarm, refer to the "Minor Network Time Protocol Service Failure - Audit (13)" section on page 2-18.

DESCRIPTION	Minor Network Time Protocol Service 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 (14)

To monitor and correct the cause of the event, refer to the "Network Time Protocol Service Warning - Audit (14)" section on page 2-15.

DESCRIPTION	Network Time Protocol Service Warning
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.

AUDIT (15)

To troubleshoot and correct the cause of the alarm, refer to the "Critical Index Shared Memory Error - Audit (15)" section on page 2-18.

DESCRIPTION	Critical Index Shared Memory Error
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 (16)

To troubleshoot and correct the cause of the alarm, refer to the "Process Heap Memory Usage Exceeds Minor Threshold Level - Audit (16)" section on page 2-18.

DESCRIPTION	Process Heap Memory Usage Exceeds Minor Threshold Level
SEVERITY	MINOR
THRESHOLD	100
THROTTLE	0
DATAWORDS	Process Name - STRING [10] Heap Size in KB - FOUR_BYTES Heap Limit in KB - FOUR_BYTES Heap Usage Percentage - FOUR_BYTES Threshold Level Percentage - FOUR_BYTES
PRIMARY CAUSE	Increase in heap usage due to high call traffic or maintenance operation.
PRIMARY ACTION	Monitor heap usage frequently and see whether it is approaching major threshold level.

AUDIT (17)

To troubleshoot and correct the cause of the alarm, refer to the "Process Heap Memory Usage Exceeds Major Threshold Level - Audit (17)" section on page 2-18.

DESCRIPTION	Process Heap Memory Usage Exceeds Major Threshold Level
SEVERITY	MAJOR
THRESHOLD	100
THROTTLE	0
DATAWORDS	Process Name - STRING [10] Heap Size in KB - FOUR_BYTES Heap Limit in KB - FOUR_BYTES Heap Usage Percentage - FOUR_BYTES Threshold Level Percentage - FOUR_BYTES
PRIMARY CAUSE	Increase in heap usage due to high call traffic or maintenance operation or software problem.
PRIMARY ACTION	Schedule a switchover during maintenance window.

AUDIT (18)

To troubleshoot and correct the cause of the alarm, refer to the "Process Heap Memory Usage Exceeds Critical Threshold Level - Audit (18)" section on page 2-19.

DESCRIPTION	Process Heap Memory Usage Exceeds Critical Threshold Level
SEVERITY	CRITICAL
THRESHOLD	100
THROTTLE	0
DATAWORDS	Process Name - STRING [10] Heap Size in KB - FOUR_BYTES Heap Limit in KB - FOUR_BYTES Heap Usage Percentage - FOUR_BYTES Threshold Level Percentage - FOUR_BYTES
PRIMARY CAUSE	Increase in heap usage due to high call traffic or maintenance operation or software problem.
PRIMARY ACTION	Schedule a switchover during maintenance window as soon as possible.

AUDIT (19)

To monitor and correct the cause of the event, refer to the "Recovered Memory of Stale Call - Audit (19)" section on page 2-16.

DESCRIPTION	Recovered Memory of Stale Call
SEVERITY	WARNING
THRESHOLD	20
THROTTLE	0
DATAWORDS	Stale Memory Release Info - STRING [128]
PRIMARY CAUSE	Loss of communication with originating or terminating side.
PRIMARY ACTION	Check if adjacent network element is up and having proper communication link with softswitch.
SECONDARY CAUSE	Adjacent network device protocol error.
SECONDARY ACTION	Check the adjacent network device protocol compatibility.
TERNARY CAUSE	An internal software error has occurred.
TERNARY ACTION	Contact Cisco Support. (Contact Cisco TAC.)

Refer to the "Obtaining Documentation and Submitting a Service Request" section on page liii for detailed instructions on contacting Cisco TAC and opening a service request.

AUDIT (20)

To troubleshoot and correct the cause of the alarm, refer to the "Audit Found Lost Call Data Record - Audit (20)" section on page 2-19.

DESCRIPTION	Audit Found Lost Call Data Record
SEVERITY	MAJOR
THRESHOLD	20
THROTTLE	0
DATAWORDS	Error Text - STRING [200]
PRIMARY CAUSE	Software error - however, the orphaned records are recovered on detection 2d.
PRIMARY ACTION	Contact Cisco Support (Contact Cisco TAC.)

Refer to the "Obtaining Documentation and Submitting a Service Request" section on page liii for detailed instructions on contacting Cisco TAC and opening a service request.

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
AUDIT(9)	Softswitch Audit SIP CCB Release - Audit (9)	WARNING
AUDIT(10)	Memory Audit Complete Status - Audit (10)	INFO
AUDIT(11)	Critical Network Time Protocol Service Failure - Audit (11)	CRITICAL
AUDIT(12)	Major Network Time Protocol Service Failure - Audit (12)	MAJOR
AUDIT(13)	Minor Network Time Protocol Service Failure - Audit (13)	MINOR
AUDIT(14)	Network Time Protocol Service Warning - Audit (14)	WARNING
AUDIT(15)	Critical Index Shared Memory Error - Audit (15)	CRITICAL
AUDIT(16)	Process Heap Memory Usage Exceeds Minor Threshold Level - Audit (16)	MINOR
AUDIT(17)	Process Heap Memory Usage Exceeds Major Threshold Level - Audit (17)	MAJOR
AUDIT(18)	Process Heap Memory Usage Exceeds Critical Threshold Level - Audit (18)	CRITICAL
AUDIT(19)	Recovered Memory of Stale Call - Audit (19)	WARNING
AUDIT(20)	Audit Found Lost Call Data Record - Audit (20)	MAJOR

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 2-17.

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 2-17.

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 2-17.

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.

Softswitch Audit SIP CCB Release - Audit (9)

The Softswitch Audit SIP CCB Release event serves as a warning that one side of the BTS 10200 was inactive. To correct the primary cause of the event, let the SIA determine whether a network error or DNS error has occurred. The secondary cause of the event is that a software error has occurred. To correct the secondary cause of the event, contact Cisco TAC. Refer to the "Obtaining Documentation and Submitting a Service Request" section on page liii for detailed instructions on contacting Cisco TAC and opening a service request.

Memory Audit Complete Status - Audit (10)

The Memory Audit Complete Status event serves as an informational alert that a SIP memory audit pass has been completed. The call data memory audit information should be checked to see if any call blocks have been cleared as a result of the audit. An investigation for root cause may be useful.

Critical Network Time Protocol Service Failure - Audit (11)

The Critical Network Time Protocol Service Failure alarm (critical) indicates that a critical Network Time Protocol (NTP) service failure has occurred. To troubleshoot and correct the cause of the Critical Network Time Protocol Service Failure alarm, refer to the "Critical Network Time Protocol Service Failure - Audit (11)" section on page 2-18.

Major Network Time Protocol Service Failure - Audit (12)

The Major Network Time Protocol Service Failure alarm (major) indicates that a major NTP service failure has occurred. To troubleshoot and correct the cause of the Major Network Time Protocol Service Failure alarm, refer to the "Major Network Time Protocol Service Failure - Audit (12)" section on page 2-18.

Minor Network Time Protocol Service Failure - Audit (13)

The Minor Network Time Protocol Service Failure alarm (minor) indicates that a minor NTP service failure has occurred. To troubleshoot and correct the cause of the Minor Network Time Protocol Service Failure alarm, refer to the "Minor Network Time Protocol Service Failure - Audit (13)" section on page 2-18.

Network Time Protocol Service Warning - Audit (14)

The Network Time Protocol Service Warning event serves as a warning that a problem with a NTP service has occurred. To correct the NTP service 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 NTP service warning sections.

Critical Index Shared Memory Error - Audit (15)

The Critical Index Shared Memory Error alarm (critical) indicates that a critical shared memory index (IDX) error has occurred. To troubleshoot and correct the cause of the Critical Index Shared Memory Error alarm, refer to the "Critical Index Shared Memory Error - Audit (15)" section on page 2-18.

Process Heap Memory Usage Exceeds Minor Threshold Level - Audit (16)

The Process Heap Memory Usage Exceeds Minor Threshold Level alarm (minor) indicates that a process heap memory usage minor threshold level crossing has occurred. To troubleshoot and correct the cause of the Process Heap Memory Usage Exceeds Minor Threshold Level alarm, refer to the "Process Heap Memory Usage Exceeds Minor Threshold Level - Audit (16)" section on page 2-18.

Process Heap Memory Usage Exceeds Major Threshold Level - Audit (17)

The Process Heap Memory Usage Exceeds Major Threshold Level alarm (major) indicates that a process heap memory usage major threshold level crossing has occurred. To troubleshoot and correct the cause of the Process Heap Memory Usage Exceeds Major Threshold Level alarm, refer to the "Process Heap Memory Usage Exceeds Major Threshold Level - Audit (17)" section on page 2-18.

Process Heap Memory Usage Exceeds Critical Threshold Level - Audit (18)

The Process Heap Memory Usage Exceeds Critical Threshold Level alarm (critical) indicates that a process heap memory usage critical threshold level crossing has occurred. To troubleshoot and correct the cause of the Process Heap Memory Usage Exceeds Critical Threshold Level alarm, refer to the "Process Heap Memory Usage Exceeds Critical Threshold Level - Audit (18)" section on page 2-19.

Recovered Memory of Stale Call - Audit (19)

The Recovered Memory of Stale Call event serves as a warning that recovery of memory from a stale call has occurred. The primary cause of the warning is that a loss of communication with originating or terminating side occurred. To correct the primary cause of the warning, check if adjacent network element link is up and that the adjacent network element is properly communicating with the Cisco BTS 10200 Softswitch. The secondary cause of the warning is that an adjacent network device has a protocol error. To correct the secondary cause of the warning, check the adjacent network device protocol compatibility with the Cisco BTS 10200 Softswitch. The ternary cause of the warning is an internal software error. If a internal software error has occurred, contact Cisco to obtain technical assistance. Refer to the "Obtaining Documentation and Submitting a Service Request" section on page liii for detailed instructions on contacting Cisco TAC and opening a service request.

Audit Found Lost Call Data Record - Audit (20)

The Audit Found Lost Call Data Record alarm (major) indicates that an audit process has found a lost call data record. To troubleshoot and correct the cause of the Audit Found Lost Call Data Record alarm, refer to the "Audit Found Lost Call Data Record - Audit (20)" section on page 2-19.

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
AUDIT(11)	Critical Network Time Protocol Service Failure - Audit (11)	CRITICAL
AUDIT(12)	Major Network Time Protocol Service Failure - Audit (12)	MAJOR
AUDIT(13)	Minor Network Time Protocol Service Failure - Audit (13)	MINOR
AUDIT(15)	Critical Index Shared Memory Error - Audit (15)	CRITICAL
AUDIT(16)	Process Heap Memory Usage Exceeds Minor Threshold Level - Audit (16)	MINOR
AUDIT(17)	Process Heap Memory Usage Exceeds Major Threshold Level - Audit (17)	MAJOR
AUDIT(18)	Process Heap Memory Usage Exceeds Critical Threshold Level - Audit (18)	CRITICAL
AUDIT(20)	Audit Found Lost Call Data Record - Audit (20)	MAJOR

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.

Critical Network Time Protocol Service Failure - Audit (11)

The Critical Network Time Protocol Service Failure alarm (critical) indicates that a critical NTP service 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 Network Time Protocol Service Failure - Audit (12)

The Major Network Time Protocol Service Failure alarm (major) indicates that a major NTP service 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 Network Time Protocol Service Failure - Audit (13)

The Minor Network Time Protocol Service Failure alarm (minor) indicates that a minor NTP service 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.

Critical Index Shared Memory Error - Audit (15)

The Critical Index Shared Memory Error alarm (critical) indicates that a critical shared memory index error 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.

Process Heap Memory Usage Exceeds Minor Threshold Level - Audit (16)

The Process Heap Memory Usage Exceeds Minor Threshold Level alarm (minor) indicates that a process heap memory usage minor threshold level crossing has occurred. The primary cause of the alarm is that the increase in heap usage is due to a high call volume of traffic or a maintenance operation. Frequently monitor heap usage and see whether it is approaching major threshold level.

Process Heap Memory Usage Exceeds Major Threshold Level - Audit (17)

The Process Heap Memory Usage Exceeds Major Threshold Level alarm (major) indicates that a process heap memory usage major threshold level crossing has occurred. The primary cause of the alarm is that the increase in heap usage is due to a high call volume of traffic, a maintenance operation, a software problem. To isolate and correct the primary cause of the alarm, schedule a switchover during a maintenance window.

Process Heap Memory Usage Exceeds Critical Threshold Level - Audit (18)

The Process Heap Memory Usage Exceeds Critical Threshold Level alarm (critical) indicates that a process heap memory usage critical threshold level crossing has occurred. The primary cause of the alarm is that the increase in heap usage is due to a high call volume of traffic, a maintenance operation, a software problem. To isolate and correct the primary cause of the alarm, schedule a switchover during a maintenance window as soon as possible.

Audit Found Lost Call Data Record - Audit (20)

The Audit Found Lost Call Data Record alarm (major) indicates that an audit process has found a lost call data record. The primary cause of the alarm is that a software error has occurred; however, the orphaned records are recovered on detection 2d. To correct the primary cause of the alarm, contact Cisco TAC. Refer to the "Obtaining Documentation and Submitting a Service Request" section on page liii for detailed instructions on contacting Cisco TAC and opening a service request.

CHAPTER 3

Billing Troubleshooting

Revised: July 22, 2009, OL-8000-32

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 (40)	BILLING (42)	BILLING (5)
BILLING (13)	BILLING (8)	BILLING (41)		BILLING (36)
BILLING (35)	BILLING (15)	BILLING (47)		BILLING (44)
BILLING (49)	BILLING (29)	BILLING (53)		BILLING (45)
BILLING (52)	BILLING (30)			BILLING (46)
BILLING (55)	BILLING (31)			BILLING (57)
BILLING (56)	BILLING (32)			
	BILLING (33)			
	BILLING (37)			
	BILLING (38)			
	BILLING (48)			
	BILLING (54)			
	BILLING (58)			
	BILLING (60)			

BILLING (1)

For additional information, refer to the "Test Report - Billing (1)" section on page 3-24.

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 3-32.

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 3-32.

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 Documentation and Submitting a Service Request" section on page liii 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 3-32.

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 Documentation and Submitting a Service Request" section on page liii 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 3-24.

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 3-33.

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
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.
SUBSEQUENT CAUSE	The CDB_BILLING_SUPP flag is not set to "Y" in the call-agent-profile table.
SUBSEQUENT ACTION	Check and verify that the CDB_BILLING_SUPP flag is set to "Y" in the call-agent-profile table.

BILLING (7)

To troubleshoot and correct the cause of the alarm, refer to the "Transmission Control Protocol Connection Error - Billing (7)" section on page 3-34.

DESCRIPTION	Transmission Control Protocol 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 Documentation and Submitting a Service Request" section on page liii 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 3-34.

DESCRIPTION	Transmission Control Protocol 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 3-34.

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 Documentation and Submitting a Service Request" section on page liii 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 3-25.

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 Documentation and Submitting a Service Request" section on page liii 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 3-34.

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 Documentation and Submitting a Service Request" section on page liii 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 3-35.

DESCRIPTION	Call Data Block 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 blg and bmg processes in 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 3-35.

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 opticall.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 3-35.

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 3-35.

DESCRIPTION	Element Management System 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 3-35.

DESCRIPTION	File Transfer Protocol/Secure File Transfer Protocol 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 3-36.

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	Do a "ifconfig up".

BILLING (36)

For additional information, refer to the "Billing Link Restored - Billing (36)" section on page 3-27.

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 3-36.

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 "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 3-36.

DESCRIPTION	Event Message Log File Access Error
SEVERITY	MAJOR
THRESHOLD	50
THROTTLE	0
DATAWORDS	Type of Access Error - STRING [25] Reason for Error - STRING [40] Sequence Number of F - 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 Documentation and Submitting a Service Request" section on page liii for detailed instructions on contacting Cisco TAC and opening a service request.

Note BILLING (39) is not used.

BILLING (40)

To troubleshoot and correct the cause of the alarm, refer to the "Event Message Encode Failure - Billing (40)" section on page 3-36.

DESCRIPTION	Event Message 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 Documentation and Submitting a Service Request" section on page liii 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 3-36.

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 Documentation and Submitting a Service Request" section on page liii 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 3-27.

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 Documentation and Submitting a Service Request" section on page liii 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 3-37.

DESCRIPTION	Record Keeping System 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 3-37.

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 3-37.

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 3-37.

DESCRIPTION	Record Keeping System Unreachable for One 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 3-37.

DESCRIPTION	Record Keeping System Unreachable for Three 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 severs 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 3-38.

DESCRIPTION	Record Keeping System 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 (50) and BILLING (51) 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 3-38.

DESCRIPTION	Bulk Data Management System 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 3-38.

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 3-38.

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 3-38.

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 3-39.

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 Documentation and Submitting a Service Request" section on page liii 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 3-29.

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 3-39.

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.

Note BILLING (59) is not used.

BILLING (60)

To troubleshoot and correct the cause of the alarm, refer to the "Bad File Detected During Startup - Billing (60)" section on page 3-39.

DESCRIPTION	Bad File Detected During Startup
SEVERITY	MAJOR
THRESHOLD	100
THROTTLE	0
DATAWORDS	File-name of the Bad File - STRING [128] Diagnosis - STRING [64] Changed to File-name - STRING [128]
PRIMARY CAUSE	A bad billing file was generated due to a CPU fatal, power outage, ungraceful shutdown, or disk failure.
PRIMARY ACTION	The Billing subsysterm will isolate the bad file, rename the bad billing file, and continue to complete the initialization. The bad file is now out of the control by Billing subsystem and it will not FTP to the BMS. The bad file should either be deleted or the content of the file should be corrected and then the file should be uploaded to the BMS.

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

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

Event Type	Event Name	Event Severity
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
BILLING(60)	Bad File Detected During Startup - Billing (60)	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 3-32.

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 3-32.

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 3-32.

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 3-33.

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 3-34.

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 3-34.

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 3-34.

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 Documentation and Submitting a Service Request" section on page liii 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 3-34.

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 3-35.

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 3-35.

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 3-35.

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 3-35.

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 3-35.

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 3-36.

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 3-36.

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 3-36.

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 3-36.

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 3-36.

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 Documentation and Submitting a Service Request" section on page liii 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 3-37.

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 3-37.

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 3-37.

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 3-37.

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 3-37.

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 3-38.

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 3-38.

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 3-38.

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 3-38.

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 3-38.

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 3-39.

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 3-39.

Bad File Detected During Startup - Billing (60)

The Bad File Detected During Startup alarm (major) indicates that a bad file was detected during system startup. To troubleshoot and correct the cause of the Bad File Detected During Startup alarm, refer to the "Bad File Detected During Startup - Billing (60)" section on page 3-39.

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(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(60)	Bad File Detected During Startup - Billing (60)	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 Documentation and Submitting a Service Request" section on page liii 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 Documentation and Submitting a Service Request" section on page liii 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 ternary cause of the alarm is that a file transfer error occurred. To correct the ternary 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 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 Documentation and Submitting a Service Request" section on page liii 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 Documentation and Submitting a Service Request" section on page liii 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 Documentation and Submitting a Service Request" section on page liii 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 he 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 opticall.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 Documentation and Submitting a Service Request" section on page liii 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.

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 Documentation and Submitting a Service Request" section on page liii 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 Documentation and Submitting a Service Request" section on page liii 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 Documentation and Submitting a Service Request" section on page liii 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.

Bad File Detected During Startup - Billing (60)

The Bad File Detected During Startup alarm (major) indicates that a bad file was detected during startup. The primary cause of the alarm is that a bad billing file was generated due to a CPU fatal, power outage, ungraceful shutdown, or disk failure. To correct the primary cause of the alarm, delete the bad file or correct the content of the file and upload the corrected file to the BMS system. If the bad file is not deleted or correct, it will remain on the system and it will not be automatically FTP'd to the BMS system.

CHAPTER 4

Call Processing Troubleshooting

Revised: July 22, 2009, OL-8000-32

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 (41)	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 (40)	

CALLP (1)

For additional information, refer to the "Test Report - Call Processing (1)" section on page 4-21.

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

Note Call processing (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 4-21.

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 4-21.

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 CCALLP (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 4-27.

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 4-29.

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 4-22.

DESCRIPTION	Network Access Server Create Connection 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 4-22.

DESCRIPTION	Network Access Server 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 4-22.

DESCRIPTION	Cable Modem Termination System Easily Recognizable Identification Not Found in Media Gateway 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 4-22.

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 4-22.

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 4-23.

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 4-23.

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 4-23.

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 4-23.

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 4-23.

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 4-23.

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 4-24.

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 4-24.

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 4-24.

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 4-24.

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 4-24.

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 4-24.

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 4-25.

DESCRIPTION	Customer-Originated Trace 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 Documentation and Submitting a Service Request" section on page liii 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 4-25.

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 Documentation and Submitting a Service Request" section on page liii 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 4-25.

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 4-25.

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 4-25.

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 4-25.

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 4-26.

DESCRIPTION	Invalid or Unknown Nature of Address
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 4-26.

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 Documentation and Submitting a Service Request" section on page liii 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 4-30.

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 4-26.

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.

CALLP (40)

To monitor and correct the cause of the event, refer to the "Interactive Voice Response Real Time Transport Protocol Session Fail - Call Processing (40)" section on page 4-26.

DESCRIPTION	Interactive Voice Response Real Time Transport Protocol Session Fail
SEVERITY	WARNING
THRESHOLD	100
THROTTLE	0
DATAWORDS	Route Guide ID - STRING [17] Trunk Group Index - FOUR_BYTES
PRIMARY CAUSE	The interactive voice response (IVR) server is not ready, or the connection failed.
PRIMARY ACTION	Check IVR server. The related route guide ID and/or trunk group index are provided if known at the time the event report is issued.

CALLP (41)

To troubleshoot and correct the cause of the alarm, refer to the "INVITE Message From Unauthorized Call Agent - Call Processing (41)" section on page 4-30.

DESCRIPTION	INVITE Message From Unauthorized Call Agent
SEVERITY	MINOR
THRESHOLD	100
THROTTLE	0
DATAWORDS	Unauthorized Call Agent DN - STRING [128] Platform Name - STRING [32]
PRIMARY CAUSE	CALL-AGENT table is not configured properly.
PRIMARY ACTION	Reconfigure the CALL-AGENT table to have the authorized call agent (CA).
SECONDARY CAUSE	Potential intrusion if the network-ID mismatch from local-network.
SECONDARY ACTION	Configure the network to block this unauthorized network-ID.

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

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

Event Type	Event Name	Event Severity
CALLP(39)	Test Call Blocked Due to Congestion or Isolation - Call Processing (39)	WARNING
CALLP(40)	Interactive Voice Response Real Time Transport Protocol Session Fail - Call Processing (40)	WARNING
CALLP(41)	INVITE Message From Unauthorized Call Agent - Call Processing (41)	MINOR

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 4-27.

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 4-29.

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. The 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 Documentation and Submitting a Service Request" section on page liii 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 Documentation and Submitting a Service Request" section on page liii 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 Documentation and Submitting a Service Request" section on page liii 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 4-30.

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

Interactive Voice Response Real Time Transport Protocol Session Fail - Call Processing (40)

The Interactive Voice Response Real Time Transport Protocol Session Fail event functions as a warning that the IVR Real Time Transport Protocol (RTP) session failed. The primary cause of the event is that the IVR server is not ready, or the connection failed. To correct the primary cause of the event, check IVR server. The related route guide ID and/or trunk group index are provided if known at the time the event report is issued

INVITE Message From Unauthorized Call Agent - Call Processing (41)

The INVITE Message From Unauthorized Call Agent alarm (minor) indicates that a INVITE message was received from an unauthorized CA. To troubleshoot and correct the cause of the INVITE Message From Unauthorized Call Agent alarm, refer to the "INVITE Message From Unauthorized Call Agent - Call Processing (41)" section on page 4-30.

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
CALLP(41)	INVITE Message From Unauthorized Call Agent - Call Processing (41)	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 the 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 the 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

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 4-25 for additional troubleshooting information.

INVITE Message From Unauthorized Call Agent - Call Processing (41)

The INVITE Message From Unauthorized Call Agent alarm (minor) indicates that a INVITE message was received from an unauthorized CA. The primary cause of the alarm is that the Call-Agent Table is not configured properly. To correct the primary cause of the alarm, reconfigure the Call-Agent table to have the authorized CA listed. The secondary cause of the alarm is that a potential intrusion occurred if the Network-ID mismatch is from the local-network. To correct the secondary cause of the alarm, configure the network to block this unauthorized Network-ID.

CHAPTER 5

Configuration Troubleshooting

Revised: July 22, 2009, OL-8000-32

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
CONFIG (4)	CONFIG (3)	CONFIG (5)		CONFIG (1)
				CONFIG (2)

CONFIG (1)

For additional information, refer to the "Test Report - Configuration (1)" section on page 5-5.

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 5-5.

DESCRIPTION	Signaling Media Gateway Adapter Wrongly Configured Domain Name
SEVERITY	INFO
THRESHOLD	1
THROTTLE	1
DATAWORDS	Configured Domain Na - STRING [256] 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 5-7.

DESCRIPTION	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 5-7.

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.

CONFIG (5)

To troubleshoot and correct the cause of the alarm, refer to the "Feature-Server Database and Command Line Host Mismatch - Configuration (5)" section on page 5-7.

DESCRIPTION	Feature-Server Database and Command Line Host Mismatch
SEVERITY	MINOR
THRESHOLD	100
THROTTLE	0
DATAWORDS	Command Line DN - STRING [128] Feature-Server DN - STRING [128] Platform Name - STRING [32]
PRIMARY CAUSE	The Feature-Server table is mis-configured.
PRIMARY ACTION	Reconfigure the Feature-Server table to match command line -host & -port.

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)	Test Report - Configuration (1)	INFO
CONFIG(2)	Signaling Media Gateway Adapter Wrongly Configured Domain Name - Configuration (2)	INFO
CONFIG(3)	Mate Configuration Error - Configuration (3)	MAJOR
CONFIG(4)	Configuration Error - Configuration (4)	CRITICAL
CONFIG(5)	Feature-Server Database and Command Line Host Mismatch - Configuration (5)	MINOR

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 5-7.

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 5-7.

Feature-Server Database and Command Line Host Mismatch - Configuration (5)

The Feature-Server Database and Command Line Host Mismatch alarm (minor) indicates that a feature-server database (DB) and host command line mismatch configuration error has occurred. To troubleshoot and correct the cause of the Feature-Server Database and Command Line Host Mismatch alarm, refer to the "Feature-Server Database and Command Line Host Mismatch - Configuration (5)" section on page 5-7.

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)	Mate Configuration Error - Configuration (3)	MAJOR
CONFIG(4)	Configuration Error - Configuration (4)	CRITICAL
CONFIG(5)	Feature-Server Database and Command Line Host Mismatch - Configuration (5)	MINOR

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.

Feature-Server Database and Command Line Host Mismatch - Configuration (5)

The Feature-Server Database and Command Line Host Mismatch alarm (minor) indicates that a feature-server DB and host command line mismatch configuration error has occurred. The primary cause of the alarm is that the Feature-Server Table is mis-configured. To correct the primary cause of the alarm, reconfigure the Feature-Server table configuration to match command line -host and -port.

CHAPTER 6

Database Troubleshooting

Revised: July 22, 2009, OL-8000-32

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
DATABASE (3)	DATABASE (6)	DATABASE (7)	DATABASE (2)	DATABASE (1)
DATABASE (4)	DATABASE (8)	DATABASE (14)	DATABASE (18)	DATABASE (19)
DATABASE (5)	DATABASE (10)	DATABASE (21)		
DATABASE (9)	DATABASE (11)			
DATABASE (12)	DATABASE (13)			
DATABASE (16)	DATABASE (15)			
	DATABASE (17)			
	DATABASE (20)			
	DATABASE (25)			
	DATABASE (26)			

DATABASE (1)

For additional information, refer to the "Test Report - Database (1)" section on page 6-17.

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 6-18.

DESCRIPTION	Database Management Update Failure: Master/Slave Database Out of Sync
SEVERITY	WARNING
THRESHOLD	100
THROTTLE	0
DATAWORDS	Error Code - TWO_BYTES Error String - STRING [20] 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 6-23.

DESCRIPTION	There Are Errors in Element Management System Database DefError Queue; Contact Database Administrator
SEVERITY	CRITICAL
THRESHOLD	100
THROTTLE	0
DATAWORDS	Host Name - STRING [30] Database Name - STRING [10] Error Count - ONE_BYTE 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 Documentation and Submitting a Service Request" section on page liii 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 6-23.

DESCRIPTION	Element Management System Database HeartBeat: Replication PUSH Job Broken
SEVERITY	CRITICAL
THRESHOLD	100
THROTTLE	0
DATAWORDS	Host Name - STRING [30] Local Database - STRING [10] Remote Database - STRING [10] Job - STRING [5] 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 6-23.

DESCRIPTION	Element Management System Database HeartBeat Process Died
SEVERITY	CRITICAL
THRESHOLD	100
THROTTLE	0
DATAWORDS	Host Name - STRING [30] Database Name - STRING [10] 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 6-24.

DESCRIPTION	Element Management System Database Replication DefTranDest Queue Overloaded
SEVERITY	MAJOR
THRESHOLD	100
THROTTLE	0
DATAWORDS	Host Name - STRING [30] Database Name - STRING [10] Threshold - FOUR_BYTES 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 6-24.

DESCRIPTION	Element Management System Database DefTran Queue is Overloaded
SEVERITY	MINOR
THRESHOLD	100
THROTTLE	0
DATAWORDS	Host Name - STRING [30] Database Name - STRING [10] Threshold - TWO_BYTES 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 6-24.

DESCRIPTION	Element Management System Database Tablespace is Out of Free Space
SEVERITY	MAJOR
THRESHOLD	100
THROTTLE	0
DATAWORDS	Host Name - STRING [30] Database Name - STRING [10] Tablespace Name - STRING [30] Total Free Space - TWO_BYTES 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 6-24.

DESCRIPTION	Urgent: Element Management System Database Archive Log Directory is Getting Full
SEVERITY	CRITICAL
THRESHOLD	100
THROTTLE	0
DATAWORDS	Host Name - STRING [30] Database Name - STRING [10] Directory Name - STRING [100] Free Space - TWO_BYTES 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 6-24.

DESCRIPTION	Element Management System Database: Backup Fails
SEVERITY	MAJOR
THRESHOLD	100
THROTTLE	0
DATAWORDS	Host Name - STRING [30] Database Name - STRING [10] Message 1 - STRING [200] Message 2 - STRING [200] 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 6-25.

DESCRIPTION	Element Management System Database Alert.log Alerts
SEVERITY	MAJOR
THRESHOLD	100
THROTTLE	0
DATAWORDS	Host Name - STRING [30] Database Name - STRING [10] Message 1 - STRING [200] Message 2 - STRING [200] Time Stamp - STRING [20]
PRIMARY CAUSE	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.
PRIMARY ACTION	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. (Contact Cisco TAC.)

Refer to the "Obtaining Documentation and Submitting a Service Request" section on page liii 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 6-25.

DESCRIPTION	Element Management System Database Process Died
SEVERITY	CRITICAL
THRESHOLD	100
THROTTLE	0
DATAWORDS	Host Name - STRING [30] Database Name - STRING [10] Error Source - STRING [40] Message - STRING [200] 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 Documentation and Submitting a Service Request" section on page liii 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 6-25.

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

Refer to the "Obtaining Documentation and Submitting a Service Request" section on page liii 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 6-26.

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 Documentation and Submitting a Service Request" section on page liii 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 6-26.

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 6-26.

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 6-26.

DESCRIPTION	Data Replication Failed
SEVERITY	MAJOR
THRESHOLD	100
THROTTLE	0
DATAWORDS	Replication-Stage - STRING [40] Table Name - STRING [40] Index - FOUR_BYTES 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 6-20.

DESCRIPTION	Unexpected Runtime Data Interaction
SEVERITY	WARNING
THRESHOLD	100
THROTTLE	0
DATAWORDS	Internal/External In - STRING [10] Table Name - STRING [32] Table Entry - STRING [10] Table Field Name - STRING [32] Descriptive Data 1 - STRING [64] Descriptive Data 2 - STRING [64] Descriptive Data 3 - STRING [64] 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 Documentation and Submitting a Service Request" section on page liii 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 6-21.

DESCRIPTION	Daily Database Backup Completed Successfully
SEVERITY	INFO
THRESHOLD	0
THROTTLE	0
DATAWORDS	Host Name - STRING [60] ORACLE_SID - STRING [30] Process - STRING [60] Message 1 - STRING [100] Message 2 - STRING [100] 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 6-26.

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.

DATABASE (21)

To troubleshoot and correct the cause of the alarm, refer to the "Database Statistics Collection Exception - Database (21)" section on page 6-26.

DESCRIPTION	Database Statistics Collection Exception
SEVERITY	MINOR
THRESHOLD	100
THROTTLE	0
DATAWORDS	Host Name - STRING [30] Database Name - STRING [10] Schema Name - STRING [32] Object Name - STRING [64] Task Name - STRING [64] Exception - STRING [256]
PRIMARY CAUSE	Check the messages in the exception field to identify the cause of the error.
PRIMARY ACTION	The correction action varies and is determined by the type of exception. For more information about the ORA-xxxxx errors, execute "oerr ora xxxxx" command as oracle user.

Note DATABASE (22) through DATABASE (24) are not used.

DATABASE (25)

To troubleshoot and correct the cause of the alarm, refer to "Secure File Transfer Protocol Transfer Failed—Database (25)" section on page 6-27.

DESCRIPTION	Secure File Transfer Protocol Transfer Failed
SEVERITY	MAJOR
THRESHOLD	100
THROTTLE	0
DATAWORDS	FileName - STRING [128] Error - STRING [50]
PRIMARY CAUSE	Unable to connect between active and standby call agents.
PRIMARY ACTION	Verify communication between primary and CA. On each CA, ping the other node.
SECONDARY CAUSE	Unable to login to remote host.
SECONDARY ACTION	Verify that secure shell (SSH) keys have been pre-configured for user root on both active and standby call agents.
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 active and standby call agents.

DATABASE (26)

To troubleshoot and correct the cause of the alarm, refer to "File Write Error—Database (26)" section on page 6-27.

DESCRIPTION	File Write Error
SEVERITY	MAJOR
THRESHOLD	100
THROTTLE	0
DATAWORDS	Path Name - STRING [128]
PRIMARY CAUSE	System error, may be out of file descriptors.
PRIMARY ACTION	Call Cisco TAC technical support. (Contact Cisco TAC.)

Refer to the "Obtaining Documentation and Submitting a Service Request" section on page liii for detailed instructions on contacting Cisco TAC and opening a service request.

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)	Test Report - Database (1)	INFO
DATABASE(2)	Database Management Update Failure: Master/Slave Database Out of Sync - Database (2)	WARNING
DATABASE(3)	There are Errors in Element Management System Database DefError Queue; Contact Database Administrator - Database (3)	CRITICAL
DATABASE(4)	Element Management System Database HeartBeat: Replication PUSH Job Broken - Database (4)	CRITICAL
DATABASE(5)	Element Management System Database HeartBeat Process Died - Database (5)	CRITICAL
DATABASE(6)	Element Management System Database Replication DefTranDest Queue Overloaded - Database (6)	MAJOR
DATABASE(7)	Element Management System Database DefTran Queue is Overloaded - Database (7)	MINOR
DATABASE(8)	Element Management System Database Tablespace is Out of Free Space - Database (8)	MAJOR
DATABASE(9)	Urgent: Element Management System Database Archive Log Directory is Getting Full - Database (9)	CRITICAL
DATABASE(10)	Element Management System Database: Backup Fails - Database (10)	MAJOR
DATABASE(11)	Element Management System Database Alert.log Alerts - Database (11)	MAJOR
DATABASE(12)	Element Management System Database Process Died - Database (12)	CRITICAL
DATABASE(13)	Element Management System Database Performance Alert - Database (13)	MAJOR
DATABASE(14)	Table Size Exceeds Minor Threshold Limit - Database (14)	MINOR
DATABASE(15)	Table Size Exceeds Major Threshold Limit - Database (15)	MAJOR
DATABASE(16)	Table Size Exceeds Critical Threshold Limit - Database (16)	CRITICAL
DATABASE(17)	Data Replication Failed - Database (17)	MAJOR
DATABASE(18)	Unexpected Runtime Data Interaction - Database (18)	WARNING
DATABASE(19)	Daily Database Backup Completed Successfully - Database (19)	INFO
DATABASE(20)	Replication Data Flush Timeout During Switchover - Database (20)	MAJOR
DATABASE(21)	Database Statistics Collection Exception - Database (21)	MINOR
DATABASE(25)	Secure File Transfer Protocol Transfer Failed—Database (25)	MAJOR
DATABASE(26)	File Write Error—Database (26)	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 6-23.

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 6-23.

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 6-23.

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 6-24.

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 6-24.

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 6-24.

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 6-24.

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 6-24.

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 6-25.

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 6-25.

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 6-25.

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 6-26.

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 6-26.

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 6-26.

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 6-26.

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 Documentation and Submitting a Service Request" section on page liii 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 6-26.

Database Statistics Collection Exception - Database (21)

The Database Statistics Collection Exception alarm (minor) indicates that the database statistics collection process had an exception. To troubleshoot and correct the cause of the Database Statistics Collection Exception alarm, refer to the "Database Statistics Collection Exception - Database (21)" section on page 6-26.

Secure File Transfer Protocol Transfer Failed—Database (25)

The Secure File Transfer Protocol Transfer Failed alarm (alarm) indicates that a SFTP file transfer had failed. To troubleshoot and correct the cause of the Secure File Transfer Protocol Transfer Failed alarm, refer to the "Secure File Transfer Protocol Transfer Failed—Database (25)" section on page 6-27.

File Write Error—Database (26)

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—Database (26)" section on page 6-27.

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)	There Are Errors in Element Management System Database DefError Queue; Contact Database Administrator - Database (3)	CRITICAL
DATABASE(4)	Element Management System Database HeartBeat: Replication PUSH Job Broken - Database (4)	CRITICAL
DATABASE(5)	Element Management System Database HeartBeat Process Died - Database (5)	CRITICAL
DATABASE(6)	Element Management System Database Replication DefTranDest Queue Overloaded - Database (6)	MAJOR
DATABASE(7)	Element Management System Database DefTran Queue is Overloaded - Database (7)	MINOR
DATABASE(8)	Element Management System Database Tablespace is Out of Free Space - Database (8)	MAJOR
DATABASE(9)	Urgent: Element Management System Database Archive Log Directory is Getting Full - Database (9)	CRITICAL
DATABASE(10)	Element Management System Database: Backup Fails - Database (10)	MAJOR
DATABASE(11)	Element Management System Database Alert.log Alerts - Database (11)	MAJOR
DATABASE(12)	Element Management System Database Process Died - Database (12)	CRITICAL
DATABASE(13)	Element Management System Database Performance Alert - Database (13)	MAJOR
DATABASE(14)	Table Size Exceeds Minor Threshold Limit - Database (14)	MINOR
DATABASE(15)	Table Size Exceeds Major Threshold Limit - Database (15)	MAJOR
DATABASE(16)	Table Size Exceeds Critical Threshold Limit - Database (16)	CRITICAL
DATABASE(17)	Data Replication Failed - Database (17)	MAJOR
DATABASE(20)	Replication Data Flush Timeout During Switchover - Database (20)	MAJOR
DATABASE(21)	Database Statistics Collection Exception - Database (21)	MINOR
DATABASE(25)	Secure File Transfer Protocol Transfer Failed—Database (25)	MAJOR
DATABASE(26)	File Write Error—Database (26)	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 Documentation and Submitting a Service Request" section on page liii 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

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 Documentation and Submitting a Service Request" section on page liii for detailed instructions on contacting Cisco TAC and opening a service request.

Note On rare occasions, the Database (11) alarm may report ORA-01595 and ORA-01594 errors in the alert.log file. These are not errors but Oracle reporting bugs that will be corrected in a future Oracle release. Oracle takes care of the internal processing contention automatically. There is no interruption to normal application operations and no loss of data. ORA-01595 and ORA-01594 errors can occur during concurrent processing situations that have long running transactions and other small transactions.

When the Database(11) alarm is reported with ORA-01595 and ORA-01594 errors, the database administrator should manually clear the alarm from CLI.

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 Documentation and Submitting a Service Request" section on page liii 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 Documentation and Submitting a Service Request" section on page liii 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 Documentation and Submitting a Service Request" section on page liii 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.

Database Statistics Collection Exception - Database (21)

The Database Statistics Collection Exception alarm (minor) indicates that the database statistics collection process had an exception. To identify the primary cause of the alarm, check the information listed in the "Exception" dataword field. The correction action varies and is determined by the type of exception. For more information about the ORA-xxxxx errors, execute an **oerr ora xxxxx** command as an Oracle user.

Secure File Transfer Protocol Transfer Failed—Database (25)

The Secure File Transfer Protocol Transfer Failed alarm (major) indicates that a secure file transfer has failed. The primary cause of the alarm is that the SFTP was unable to connect between active and standby call agents. To troubleshoot and correct the primary cause of the alarm, verify communication between primary and secondary call agent (CA). On each CA, ping the other node. The secondary cause of the alarm is that the system was unable to login to the remote host. To troubleshoot and correct the secondary cause of the alarm, verify that the SSH keys have been pre-configured for user root on both active and standby call agents. The ternary cause of the alarm is that a file transfer error has occurred. To troubleshoot and correct the ternary 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 active and standby call agents.

File Write Error—Database (26)

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 and that the system may be out of file descriptors. To troubleshoot and correct the primary cause of the alarm, call Cisco TAC technical support.

Refer to the "Obtaining Documentation and Submitting a Service Request" section on page liii for detailed instructions on contacting Cisco TAC and opening a service request.

CHAPTER 7

Maintenance Troubleshooting

Revised: July 22, 2009, OL-8000-32

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
MAINTENANCE (40)	MAINTENANCE (3)	MAINTENANCE (18)	MAINTENANCE (29)	MAINTENANCE (1)
MAINTENANCE (43)	MAINTENANCE (4)	MAINTENANCE (24)	MAINTENANCE (41)	MAINTENANCE (2)
MAINTENANCE (44)	MAINTENANCE (5)	MAINTENANCE (48)	MAINTENANCE (75)	MAINTENANCE (11)
MAINTENANCE (47)	MAINTENANCE (6)	MAINTENANCE (67)	MAINTENANCE (105)	MAINTENANCE (12)
MAINTENANCE (50)	MAINTENANCE (7)	MAINTENANCE (83)	MAINTENANCE (106)	MAINTENANCE (13)
MAINTENANCE (53)	MAINTENANCE (8)	MAINTENANCE (86)	MAINTENANCE (108)	MAINTENANCE (14)
MAINTENANCE (57)	MAINTENANCE (9)	MAINTENANCE (90)	MAINTENANCE (123)	MAINTENANCE (15)
MAINTENANCE (61)	MAINTENANCE (10)	MAINTENANCE (98)		MAINTENANCE (16)
MAINTENANCE (65)	MAINTENANCE (19)			MAINTENANCE (17)
MAINTENANCE (69)	MAINTENANCE (20)			MAINTENANCE (22)
MAINTENANCE (70)	MAINTENANCE (21)			MAINTENANCE (25)
MAINTENANCE (73)	MAINTENANCE (23)			MAINTENANCE (27)
MAINTENANCE (74)	MAINTENANCE (26)			MAINTENANCE (28)
MAINTENANCE (82)	MAINTENANCE (42)			MAINTENANCE (30)
MAINTENANCE (85)	MAINTENANCE (45)			MAINTENANCE (32)
MAINTENANCE (91)	MAINTENANCE (49)			MAINTENANCE (33)
MAINTENANCE (97)	MAINTENANCE (51)			MAINTENANCE (34)
MAINTENANCE (100)	MAINTENANCE (55)			MAINTENANCE (35)
MAINTENANCE (101)	MAINTENANCE (62)			MAINTENANCE (36)
MAINTENANCE (102)	MAINTENANCE (63)			MAINTENANCE (37)
MAINTENANCE (103)	MAINTENANCE (64)			MAINTENANCE (38)
MAINTENANCE (107)	MAINTENANCE (66)			MAINTENANCE (39)
MAINTENANCE (111)	MAINTENANCE (68)			MAINTENANCE (46)
MAINTENANCE (118)	MAINTENANCE (71)			MAINTENANCE (52)
MAINTENANCE (119)	MAINTENANCE (72)			MAINTENANCE (54)
	MAINTENANCE (77)			MAINTENANCE (56)
	MAINTENANCE (84)			MAINTENANCE (58)
	MAINTENANCE (87)			MAINTENANCE (78)
	MAINTENANCE (88)			MAINTENANCE (79)
	MAINTENANCE (89)			MAINTENANCE (80)
	MAINTENANCE (92)			MAINTENANCE (81)

Table 7-1 Maintenance Events and Alarms by Severity (continued)

CRITICAL	MAJOR	MINOR	WARNING	INFO
	MAINTENANCE (93)			MAINTENANCE (94)
	MAINTENANCE (99)			MAINTENANCE (95)
	MAINTENANCE (109)			MAINTENANCE (96)
	MAINTENANCE (110)			MAINTENANCE (104)
				MAINTENANCE (120)
				MAINTENANCE (122)

MAINTENANCE (1)

For additional information, refer to the "Test Report - Maintenance (1)" section on page 7-66.

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 7-66.

DESCRIPTION	Report Threshold Exceeded
SEVERITY	INFO
THRESHOLD	0
THROTTLE	0
DATAWORDS	Report Type - TWO_BYTES Report Number - TWO_BYTES 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 7-88.

DESCRIPTION	Local Side has Become Faulty
SEVERITY	MAJOR
THRESHOLD	100
THROTTLE	0
DATAWORDS	Local State - STRING [30] Mate State - STRING [30] Reason - STRING [80] 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 7-88.

DESCRIPTION	Mate Side has Become Faulty
SEVERITY	MAJOR
THRESHOLD	100
THROTTLE	0
DATAWORDS	Local State - STRING [30] Mate State - STRING [30] Reason - STRING [80] Probable Cause - STRING [80] 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 Documentation and Submitting a Service Request" section on page liii 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 7-89.

DESCRIPTION	Changeover Failure
SEVERITY	MAJOR
THRESHOLD	100
THROTTLE	0
DATAWORDS	Local State - STRING [30] 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 Documentation and Submitting a Service Request" section on page liii 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 7-89.

DESCRIPTION	Changeover Timeout
SEVERITY	MAJOR
THRESHOLD	100
THROTTLE	0
DATAWORDS	Local State - STRING [30] 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 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 Documentation and Submitting a Service Request" section on page liii 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 7-89.

DESCRIPTION	Mate Rejected Changeover
SEVERITY	MAJOR
THRESHOLD	100
THROTTLE	0
DATAWORDS	Local State - STRING [30] 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. **Note** 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 Documentation and Submitting a Service Request" section on page liii 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 7-92.

DESCRIPTION	Mate Changeover Timeout
SEVERITY	MAJOR
THRESHOLD	100
THROTTLE	0
DATAWORDS	Local State - STRING [30] 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.

Refer to the "Obtaining Documentation and Submitting a Service Request" section on page liii for detailed instructions on contacting Cisco TAC and opening a service request.

MAINTENANCE (9)

To troubleshoot and correct the cause of the alarm, refer to the "Local Initialization Failure - Maintenance (9)" section on page 7-92.

DESCRIPTION	Local Initialization Failure
SEVERITY	MAJOR
THRESHOLD	100
THROTTLE	0
DATAWORDS	Local State - STRING [30] 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 7-92.

DESCRIPTION	Local Initialization Timeout
SEVERITY	MAJOR
THRESHOLD	100
THROTTLE	0
DATAWORDS	Local State - STRING [30] 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 7-68.

DESCRIPTION	Switchover Complete
SEVERITY	INFO
THRESHOLD	100
THROTTLE	0
DATAWORDS	Local State - STRING [30] 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 7-68.

DESCRIPTION	Initialization Successful
SEVERITY	INFO
THRESHOLD	100
THROTTLE	0
DATAWORDS	Local State - STRING [30] 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 7-68.

DESCRIPTION	Administrative State Change
SEVERITY	INFO
THRESHOLD	100
THROTTLE	0
DATAWORDS	Facility Type - STRING [40] Facility ID - STRING [40] Initial Admin State - STRING [20] Target Admin State - STRING [20] 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 7-68.

DESCRIPTION	Call Agent Administrative State Change
SEVERITY	INFO
THRESHOLD	100
THROTTLE	0
DATAWORDS	Call Agent ID - STRING [40] Current Local State - STRING [40] 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 7-68.

DESCRIPTION	Feature Server Administrative State Change
SEVERITY	INFO
THRESHOLD	100
THROTTLE	0
DATAWORDS	Feature Server ID - STRING [40] Feature Server Type - STRING [40] Current Local State - STRING [20] 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 7-68.

DESCRIPTION	Process Manager: Starting Process
SEVERITY	INFO
THRESHOLD	100
THROTTLE	0
DATAWORDS	Process Name - STRING [40] Restart Type - STRING [40] Restart Mode - STRING [32] 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 7-69.

DESCRIPTION	Invalid Event Report Received
SEVERITY	INFO
THRESHOLD	100
THROTTLE	0
DATAWORDS	Report Type - TWO_BYTES Report Number - TWO_BYTES 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 Documentation and Submitting a Service Request" section on page liii 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 7-92.

DESCRIPTION	Process Manager: Process has Died
SEVERITY	MINOR
THRESHOLD	100
THROTTLE	0
DATAWORDS	Process Name - STRING [40] Process Group - FOUR_BYTES
PRIMARY CAUSE	Software problem.
PRIMARY ACTION	If problem persists, contact Cisco TAC technical support. (Contact Cisco TAC.)

Refer to the "Obtaining Documentation and Submitting a Service Request" section on page liii 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 7-92.

DESCRIPTION	Process Manager: Process Exceeded Restart Rate
SEVERITY	MAJOR
THRESHOLD	100
THROTTLE	0
DATAWORDS	Process Name - STRING [40] Restart Rate - FOUR_BYTES 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 7-93.

DESCRIPTION	Lost 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	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 7-93.

DESCRIPTION	Network Interface Down
SEVERITY	MAJOR
THRESHOLD	100
THROTTLE	0
DATAWORDS	IP Address - STRING [50]
PRIMARY CAUSE	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 7-69.

DESCRIPTION	Mate is Alive
SEVERITY	INFO
THRESHOLD	100
THROTTLE	0
DATAWORDS	Local State - STRING [30] 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 7-93.

DESCRIPTION	Process Manager: Process Failed to Complete Initialization
SEVERITY	MAJOR
THRESHOLD	100
THROTTLE	0
DATAWORDS	Process Name - STRING [40] 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 7-93.

DESCRIPTION	Process Manager: Restarting Process
SEVERITY	MINOR
THRESHOLD	100
THROTTLE	0
DATAWORDS	Process Name - STRING [40] Restart Type - STRING [40] Restart Mode - STRING [32] 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 Documentation and Submitting a Service Request" section on page liii 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 7-70.

DESCRIPTION	Process Manager: 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 7-93.

DESCRIPTION	Process Manager: Going Faulty
SEVERITY	MAJOR
THRESHOLD	100
THROTTLE	0
DATAWORDS	Reason - STRING [40]
PRIMARY CAUSE	System has been brought down/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 7-70.

DESCRIPTION	Process Manager: 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 7-70.

DESCRIPTION	Process Manager: 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 7-71.

DESCRIPTION	Administrative State Change Failure
SEVERITY	WARNING
THRESHOLD	100
THROTTLE	0
DATAWORDS	Facility Type - STRING [40] Facility Instance - STRING [40] Failure Reason - STRING [40] Initial Admin State - STRING [20] Target Admin State - STRING [20] 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 7-71.

DESCRIPTION	Element Manager State Change
SEVERITY	INFO
THRESHOLD	100
THROTTLE	0
DATAWORDS	Element Manager ID - STRING [40] Current Local State - STRING [40] 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 Event 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 7-71.

DESCRIPTION	Process Manager: Sending Go Active to Process
SEVERITY	INFO
THRESHOLD	100
THROTTLE	0
DATAWORDS	Process Name - STRING [40] 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 7-71.

DESCRIPTION	Process Manager: Sending Go Standby to Process
SEVERITY	INFO
THRESHOLD	100
THROTTLE	0
DATAWORDS	Process Name - STRING [40] 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 7-71.

DESCRIPTION	Process Manager: Sending End Process to Process
SEVERITY	INFO
THRESHOLD	100
THROTTLE	0
DATAWORDS	Process Name - STRING [40] 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 7-71.

DESCRIPTION	Process Manager: 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 7-72.

DESCRIPTION	Process Manager: Sending All Processes Init Complete to Process
SEVERITY	INFO
THRESHOLD	100
THROTTLE	0
DATAWORDS	Process Name - STRING [40] 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 7-72.

DESCRIPTION	Process Manager: Killing Process
SEVERITY	INFO
THRESHOLD	100
THROTTLE	0
DATAWORDS	Process Name - STRING [40] 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 7-72.

DESCRIPTION	Process Manager: Clearing the Database
SEVERITY	INFO
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 7-72.

DESCRIPTION	Process Manager: 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 7-94.

DESCRIPTION	Process Manager: Binary Does not Exist for Process
SEVERITY	CRITICAL
THRESHOLD	100
THROTTLE	0
DATAWORDS	Program Name - STRING [30] Executable Name - STRING [100]
PRIMARY CAUSE	Platform 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 7-72.

DESCRIPTION	Administrative State Change Successful with Warning
SEVERITY	WARNING
THRESHOLD	100
THROTTLE	0
DATAWORDS	Facility Type - STRING [40] Facility Instance - STRING [40] Initial State - STRING [20] Target State - STRING [20] Current State - STRING [20] 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 7-94.

DESCRIPTION	Number of Heartbeat Messages Received is Less Than 50% of Expected
SEVERITY	MAJOR
THRESHOLD	100
THROTTLE	0
DATAWORDS	Interface Name - STRING [50] IP Address - STRING [50] Expected HB Messages - ONE_BYTE HB Messages Received - ONE_BYTE
PRIMARY CAUSE	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 7-94.

DESCRIPTION	Process Manager: Process Failed to Come Up in Active Mode
SEVERITY	CRITICAL
THRESHOLD	100
THROTTLE	0
DATAWORDS	Process Name - STRING [40] Process Group - ONE_BYTE
PRIMARY CAUSE	Software or configuration problem.
PRIMARY ACTION	Restart the platform. If problem persists call tech support. (Contact Cisco TAC.)

Refer to the "Obtaining Documentation and Submitting a Service Request" section on page liii 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 7-94.

DESCRIPTION	Process Manager: Process Failed to Come Up in Standby Mode
SEVERITY	CRITICAL
THRESHOLD	100
THROTTLE	0
DATAWORDS	Process Name - STRING [40] Process Group - ONE_BYTE
PRIMARY CAUSE	Software or configuration problem.
PRIMARY ACTION	Restart the platform. If problem persists call tech support. (Contact Cisco TAC.)

Refer to the "Obtaining Documentation and Submitting a Service Request" section on page liii 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 7-94.

DESCRIPTION	Application Instance State Change Failure
SEVERITY	MAJOR
THRESHOLD	100
THROTTLE	0
DATAWORDS	Application Instance - STRING [20] 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 Documentation and Submitting a Service Request" section on page liii 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 7-73.

DESCRIPTION	Network Interface Restored
SEVERITY	INFO
THRESHOLD	100
THROTTLE	0
DATAWORDS	Interface Name - STRING [80] Interface IP Address - STRING [80]
PRIMARY CAUSE	Interface cable is put back/interface is put "up" using ifconfig command.
PRIMARY ACTION	No action.

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 7-95.

DESCRIPTION	Thread Watchdog Counter Expired for a Thread
SEVERITY	CRITICAL
THRESHOLD	100
THROTTLE	0
DATAWORDS	Process Name - STRING [5] Thread Type - FOUR_BYTES Thread Instance - FOUR_BYTES
PRIMARY CAUSE	Software error.
PRIMARY ACTION	None (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 7-96.

DESCRIPTION	Index Table Usage Exceeded Minor Usage Threshold Level
SEVERITY	MINOR
THRESHOLD	100
THROTTLE	0
DATAWORDS	Table Name - STRING [80] Size - FOUR_BYTES Used - FOUR_BYTES
PRIMARY CAUSE	Call traffic 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 Documentation and Submitting a Service Request" section on page liii 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 7-96.

DESCRIPTION	Index Table Usage Exceeded Major Usage Threshold Level
SEVERITY	MAJOR
THRESHOLD	100
THROTTLE	0
DATAWORDS	Table Name - STRING [80] Table Size - FOUR_BYTES Used - FOUR_BYTES
PRIMARY CAUSE	Call traffic 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 Documentation and Submitting a Service Request" section on page liii 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 7-96.

DESCRIPTION	Index Table Usage Exceeded Critical Usage Threshold Level
SEVERITY	CRITICAL
THRESHOLD	100
THROTTLE	0
DATAWORDS	Table Name - STRING [80] Table Size - FOUR_BYTES Used - FOUR_BYTES
PRIMARY CAUSE	Call traffic 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.)

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 7-96.

DESCRIPTION	A Process Exceeds 70% of Central Processing Unit Usage
SEVERITY	MAJOR
THRESHOLD	100
THROTTLE	0
DATAWORDS	Host Name - STRING [40] PID - STRING [40] Process Name - STRING [40] 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 7-74.

DESCRIPTION	Central Processing Unit Usage is Now Below the 50% Level
SEVERITY	INFO
THRESHOLD	100
THROTTLE	0
DATAWORDS	Host Name - STRING [40] PID - STRING [40] Process Name - STRING [40] 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 7-96.

DESCRIPTION	The Central Processing Unit Usage is Over 90% Busy
SEVERITY	CRITICAL
THRESHOLD	100
THROTTLE	0
DATAWORDS	Host Name - STRING [40] 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 Documentation and Submitting a Service Request" section on page liii 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 7-75.

DESCRIPTION	The Central Processing Unit has Returned to Normal Levels of Operation
SEVERITY	INFO
THRESHOLD	100
THROTTLE	0
DATAWORDS	Host Name - STRING [40] 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 7-97.

DESCRIPTION	The Five Minute Load Average is Abnormally High
SEVERITY	MAJOR
THRESHOLD	100
THROTTLE	0
DATAWORDS	Host Name - STRING [40] 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 Documentation and Submitting a Service Request" section on page liii 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 7-75.

DESCRIPTION	The Load Average has Returned to Normal Levels
SEVERITY	INFO
THRESHOLD	100
THROTTLE	0
DATAWORDS	Host Name - STRING [40] 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 7-97.

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] Memory - STRING [40] 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 Documentation and Submitting a Service Request" section on page liii 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 7-75.

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
DATAWORDS	Host Name - STRING [40] Memory - STRING [40] 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 Documentation and Submitting a Service Request" section on page liii 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 7-97.

DESCRIPTION	No Heartbeat Messages Received Through the Interface
SEVERITY	CRITICAL
THRESHOLD	100
THROTTLE	0
DATAWORDS	Interface Name - STRING [20] 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 7-97.

DESCRIPTION	Link Monitor: Interface Lost Communication
SEVERITY	MAJOR
THRESHOLD	100
THROTTLE	0
DATAWORDS	Interface Name - STRING [80] Interface IP Address - STRING [80]
PRIMARY CAUSE	Interface cable is pulled out/interface is set "down" using ifconfig command.
PRIMARY ACTION	Restore the network interface.
SECONDARY CAUSE	Interface has no connectivity to any of the machines/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 7-98.

DESCRIPTION	Outgoing Heartbeat Period Exceeded Limit
SEVERITY	MAJOR
THRESHOLD	100
THROTTLE	0
DATAWORDS	Max. HB Period (ms) - FOUR_BYTES 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 Documentation and Submitting a Service Request" section on page liii 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 7-98.

DESCRIPTION	Average Outgoing Heartbeat Period Exceeds Major Alarm Limit
SEVERITY	MAJOR
THRESHOLD	100
THROTTLE	0
DATAWORDS	Max. Avg HB Period - FOUR_BYTES 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 Documentation and Submitting a Service Request" section on page liii 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 7-98.

DESCRIPTION	Disk Partition Critically Consumed
SEVERITY	CRITICAL
THRESHOLD	100
THROTTLE	0
DATAWORDS	Directory - STRING [32] Device - STRING [32] 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 7-98.

DESCRIPTION	Disk Partition Significantly Consumed
SEVERITY	MAJOR
THRESHOLD	100
THROTTLE	0
DATAWORDS	Directory - STRING [32] Device - STRING [32] 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 7-98.

DESCRIPTION	The Free Inter-Process Communication Pool Buffers Below Minor Threshold
SEVERITY	MINOR
THRESHOLD	100
THROTTLE	0
DATAWORDS	Free IPC Pool Buffer - STRING [10] 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.

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 7-99.

DESCRIPTION	The Free Inter-Process Communication Pool Buffers Below Major Threshold
SEVERITY	MAJOR
THRESHOLD	100
THROTTLE	0
DATAWORDS	Free IPC Poll Buffer - STRING [10] 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 Documentation and Submitting a Service Request" section on page liii 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 7-99.

DESCRIPTION	The Free Inter-Process Communication Pool Buffers Below Critical Threshold
SEVERITY	CRITICAL
THRESHOLD	100
THROTTLE	0
DATAWORDS	Free IPC Poll Buffer - STRING [10] 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 Documentation and Submitting a Service Request" section on page liii 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 7-99.

DESCRIPTION	The Free Inter-Process Communication Pool Buffer Count Below Minimum Required
SEVERITY	CRITICAL
THRESHOLD	100
THROTTLE	0
DATAWORDS	Free IPC Buffer Coun - TWO_BYTES 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 Documentation and Submitting a Service Request" section on page liii 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 7-99.

DESCRIPTION	Local Domain Name System 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 7-99.

DESCRIPTION	External Domain Name System 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 7-100.

DESCRIPTION	External Domain Name System 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 7-100.

DESCRIPTION	Local Domain Name System 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 7-78.

DESCRIPTION	Mismatch of Internet Protocol Address Local Server and Domain Name System
SEVERITY	WARNING
THRESHOLD	100
THROTTLE	0
DATAWORDS	Host Name - STRING [64] IP Addr Local Server - STRING [64] 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 7-100.

DESCRIPTION	Mate Time Differs Beyond Tolerance
SEVERITY	MAJOR
THRESHOLD	100
THROTTLE	0
DATAWORDS	Max Time Difference - FOUR_BYTES 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 7-78.

DESCRIPTION	Bulk Data Management System Admin State Change
SEVERITY	INFO
THRESHOLD	100
THROTTLE	0
DATAWORDS	Application Instance - STRING [40] Local State - STRING [40] 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 7-79.

DESCRIPTION	Resource Reset
SEVERITY	INFO
THRESHOLD	100
THROTTLE	0
DATAWORDS	Resource Type - STRING [40] Resource Instance - STRING [40]
PRIMARY CAUSE	Trunk-Termination Subscriber-Termination Media Gateways
PRIMARY ACTION	None

MAINTENANCE (80)

For additional information, refer to the "Resource Reset Warning - Maintenance (80)" section on page 7-79.

DESCRIPTION	Resource Reset Warning
SEVERITY	INFO
THRESHOLD	100
THROTTLE	0
DATAWORDS	Resource Type - STRING [40] Resource Instance - STRING [40] Warning Reason - STRING [120]
PRIMARY CAUSE	Trunk-Termination Subscriber-Termination Media Gateway
PRIMARY ACTION	None

MAINTENANCE (81)

For additional information, refer to the "Resource Reset Failure - Maintenance (81)" section on page 7-79.

DESCRIPTION	Resource Reset Failure
SEVERITY	INFO
THRESHOLD	100
THROTTLE	0
DATAWORDS	Resource Type - STRING [40] Resource Instance - STRING [40] 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 7-100.

DESCRIPTION	Average Outgoing Heartbeat Period Exceeds Critical Limit
SEVERITY	CRITICAL
THRESHOLD	100
THROTTLE	0
DATAWORDS	Critical Threshold F - FOUR_BYTES 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 7-100.

DESCRIPTION	Swap Space Below Minor Threshold
SEVERITY	MINOR
THRESHOLD	5
THROTTLE	0
DATAWORDS	Minor Threshold (MB) - FOUR_BYTES Current Value (MB) - FOUR_BYTES
PRIMARY CAUSE	Too many processes.
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 7-101.

DESCRIPTION	Swap Space Below Major Threshold
SEVERITY	MAJOR
THRESHOLD	5
THROTTLE	0
DATAWORDS	Major Threshold (MB) - FOUR_BYTES Current Value (MB) - FOUR_BYTES
PRIMARY CAUSE	Too many processes.
PRIMARY ACTION	Stop proliferation of executables (processes/shell-procedures).
SECONDARY CAUSE	File spaces /tmp or /var/run 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 7-101.

DESCRIPTION	Swap Space Below Critical Threshold
SEVERITY	CRITICAL
THRESHOLD	5
THROTTLE	0
DATAWORDS	Critical Threshold (M - FOUR_BYTES Current Value (MB) - FOUR_BYTES
PRIMARY CAUSE	Too many processes.
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 7-101.

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 Documentation and Submitting a Service Request" section on page liii 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 7-101.

DESCRIPTION	Status Update Process Request Failed
SEVERITY	MAJOR
THRESHOLD	100
THROTTLE	0
DATAWORDS	ErrString - STRING [64] Component Type - STRING [64]
PRIMARY CAUSE	The "status" command 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 7-101.

DESCRIPTION	Status Update Process Database 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 Documentation and Submitting a Service Request" section on page liii 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 7-101.

DESCRIPTION	Status Update Process Database Update Error
SEVERITY	MAJOR
THRESHOLD	100
THROTTLE	0
DATAWORDS	ErrString - STRING [64] 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 Documentation and Submitting a Service Request" section on page liii 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 7-102.

DESCRIPTION	Disk Partition Moderately Consumed
SEVERITY	MINOR
THRESHOLD	100
THROTTLE	0
DATAWORDS	Directory - STRING [32] Device - STRING [32] 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 7-102.

DESCRIPTION	Internet Protocol Manager Configuration 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 7-102.

DESCRIPTION	Internet Protocol Manager Initialization Error
SEVERITY	MAJOR
THRESHOLD	100
THROTTLE	0
DATAWORDS	Reason - STRING [128]
PRIMARY CAUSE	IPM failed to initialize correctly.
PRIMARY ACTION	Check reason 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 7-102.

DESCRIPTION	Internet Protocol Manager Interface Failure
SEVERITY	MAJOR
THRESHOLD	100
THROTTLE	0
DATAWORDS	Interface Name - STRING [32] Reason - STRING [128]
PRIMARY CAUSE	IPM failed to create logical interface.
PRIMARY ACTION	Check reason as to cause of error.

MAINTENANCE (94)

For additional information, refer to the "Internet Protocol Manager Interface State Change - Maintenance (94)" section on page 7-81.

DESCRIPTION	Internet Protocol Manager Interface State Change
SEVERITY	INFO
THRESHOLD	100
THROTTLE	0
DATAWORDS	Interface Name - STRING [32] 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 7-81.

DESCRIPTION	Internet Protocol Manager Interface Created
SEVERITY	INFO
THRESHOLD	100
THROTTLE	0
DATAWORDS	Hostname - STRING [128] Physical IF Name - STRING [32] Logical IF Name - STRING [32] IP Addr - STRING [32] Netmask - STRING [32] 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 7-81.

DESCRIPTION	Internet Protocol Manager Interface Removed
SEVERITY	INFO
THRESHOLD	100
THROTTLE	0
DATAWORDS	Hostname - STRING [128] Logical IF Name - STRING [32] 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 7-102.

DESCRIPTION	Inter-Process Communication Input Queue Entered Throttle State
SEVERITY	CRITICAL
THRESHOLD	500
THROTTLE	0
DATAWORDS	Process Name - STRING [10] Thread Type - TWO_BYTES Thread Instance - TWO_BYTES Hi Watermark - FOUR_BYTES 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 Documentation and Submitting a Service Request" section on page liii 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 7-102.

DESCRIPTION	Inter-Process Communication Input Queue Depth at 25% of Its Hi-Watermark
SEVERITY	MINOR
THRESHOLD	500
THROTTLE	0
DATAWORDS	Process Name - STRING [10] Thread Type - TWO_BYTES Thread Instance - TWO_BYTES Hi Watermark - FOUR_BYTES 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 Documentation and Submitting a Service Request" section on page liii 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 7-103.

DESCRIPTION	Inter-Process Communication Input Queue Depth at 50% of Its Hi-Watermark
SEVERITY	MAJOR
THRESHOLD	500
THROTTLE	0
DATAWORDS	Process Name - STRING [10] Thread Type - TWO_BYTES Thread Instance - TWO_BYTES Hi Watermark - FOUR_BYTES 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 Documentation and Submitting a Service Request" section on page liii 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 7-103.

DESCRIPTION	Inter-Process Communication Input Queue Depth at 75% of Its Hi-Watermark
SEVERITY	CRITICAL
THRESHOLD	500
THROTTLE	0
DATAWORDS	Process Name - STRING [10] Thread Type - TWO_BYTES Thread Instance - TWO_BYTES Hi Watermark - FOUR_BYTES 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 Documentation and Submitting a Service Request" section on page liii 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 7-103.

DESCRIPTION	Switchover in Progress
SEVERITY	CRITICAL
THRESHOLD	100
THROTTLE	0
DATAWORDS	Local State - STRING [15] Mate State - STRING [15] 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 itself 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 7-103.

DESCRIPTION	Thread Watchdog Counter Close to Expiry for a Thread
SEVERITY	CRITICAL
THRESHOLD	100
THROTTLE	0
DATAWORDS	Process Name - STRING [5] Thread Type - FOUR_BYTES 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 7-104.

DESCRIPTION	Central Processing Unit is Offline
SEVERITY	CRITICAL
THRESHOLD	100
THROTTLE	0
DATAWORDS	Hostname - STRING [20] CPU - ONE_BYTE
PRIMARY CAUSE	Operator action.
PRIMARY ACTION	Restore CPU or contact Cisco TAC.

Refer to the "Obtaining Documentation and Submitting a Service Request" section on page liii for detailed instructions on contacting Cisco TAC and opening a service request.

MAINTENANCE (104)

For additional information, refer to the "Aggregation Device Address Successfully Resolved - Maintenance (104)" section on page 7-83.

DESCRIPTION	Aggregation Device Address Successfully Resolved
SEVERITY	INFO
THRESHOLD	100
THROTTLE	0
DATAWORDS	MGW IP Address - STRING [17] MGW ID - STRING [33] AGGR ID - STRING [33] Network Address - STRING [17] Subnet Mask - ONE_BYTE
PRIMARY CAUSE	Informational
PRIMARY ACTION	No action needs to be taken.

MAINTENANCE (105)

To monitor and correct the cause of the event, refer to the "Unprovisioned Aggregation Device Detected - Maintenance (105)" section on page 7-83.

DESCRIPTION	Unprovisioned Aggregation Device Detected
SEVERITY	WARNING
THRESHOLD	100
THROTTLE	0
DATAWORDS	AGGR IP address - STRING [17] MGW IP address - STRING [17] MGW ID - STRING [33]
PRIMARY CAUSE	Aggregation (AGGR) Internet Protocol (IP) address is not provisioned in aggregation table.
PRIMARY ACTION	Provisioned AGGR with AGGR IP address in AGGR table.

MAINTENANCE (106)

To monitor and correct the cause of the event, refer to the"Aggregation Device Address Resolution Failure - Maintenance (106)" section on page 7-83.

DESCRIPTION	Aggregation Device Address Resolution Failure
SEVERITY	WARNING
THRESHOLD	100
THROTTLE	0
DATAWORDS	Reason Code - STRING [17] MGW ID - STRING [33] Reason - STRING [128]
PRIMARY CAUSE	Auto AGGR-identification (ID) resolution for media gateway (MGW) IP failed due to DNS lookup failure.
PRIMARY ACTION	Check provisioning of DNS reverse lookup entry for MGW IP address.

MAINTENANCE (107)

To troubleshoot and correct the cause of the alarm, refer to the "No Heartbeat Messages Received Through Interface From Router - Maintenance (107)" section on page 7-104.

DESCRIPTION	No Heartbeat Messages Received Through Interface From Router
SEVERITY	CRITICAL
THRESHOLD	100
THROTTLE	0
DATAWORDS	Interface Name - STRING [20] Critical Local IP Address - STRING [50] Router IP Address - STRING [50]
PRIMARY CAUSE	Router is down.
PRIMARY ACTION	Restore router functionality.
SECONDARY CAUSE	Connection to router down.
SECONDARY ACTION	Restore connection.
TERNARY CAUSE	Network congestion.

MAINTENANCE (108)

To monitor and correct the cause of the event, refer to the "A Log File Cannot be Transferred - Maintenance (108)" section on page 7-83.

DESCRIPTION	A Log File Cannot be Transferred
SEVERITY	WARNING
THRESHOLD	5
THROTTLE	0
DATAWORDS	Name of the File With Full Path - STRING [100] External Archive System - STRING [50]
PRIMARY CAUSE	Problem in access to external archive system.
PRIMARY ACTION	Check the external archive system.
SECONDARY CAUSE	The network to external archive system is down.
SECONDARY ACTION	Check the network.
TERNARY CAUSE	The source log file is not present.
TERNARY ACTION	Check the presence of log file.

MAINTENANCE (109)

To troubleshoot and correct the cause of the alarm, refer to the "Five Successive Log Files Cannot be Transferred - Maintenance (109)" section on page 7-104.

DESCRIPTION	Five Successive Log Files Cannot be Transferred
SEVERITY	MAJOR
THRESHOLD	100
THROTTLE	0
DATAWORDS	External Archive Systems - STRING [100]
PRIMARY CAUSE	Problem in access to external archive system.
PRIMARY ACTION	Check the external archive system.
SECONDARY CAUSE	Network to external archive system is down.
SECONDARY ACTION	Check the network.

MAINTENANCE (110)

To troubleshoot and correct the cause of the alarm, refer to the "Access to Log Archive Facility Configuration File Failed or File Corrupted - Maintenance (110)" section on page 7-104.

DESCRIPTION	Access to Log Archive Facility Configuration File Failed or File Corrupted
SEVERITY	MAJOR
THRESHOLD	10
THROTTLE	0
DATAWORDS	Full Path of LAF Configuration F - STRING [50]
PRIMARY CAUSE	File corrupted.
PRIMARY ACTION	Check the log archive facility (LAF) configuration file.
SECONDARY CAUSE	The file is missing.
SECONDARY ACTION	Check the presence of LAF configuration file.

MAINTENANCE (111)

To troubleshoot and correct the cause of the alarm, refer to the "Cannot Login to External Archive Server - Maintenance (111)" section on page 7-104.

DESCRIPTION	Cannot Login to External Archive Server
SEVERITY	CRITICAL
THRESHOLD	10
THROTTLE	0
DATAWORDS	External Archive Server - STRING [50] Username - STRING [50]
PRIMARY CAUSE	No authorization access is set up in external archive server for that user from Cisco BTS 10200 Softswitch.
PRIMARY ACTION	Set up the authorization.
SECONDARY CAUSE	The external archive server is down.
SECONDARY ACTION	Ping the external archive server, and try to bring it up.
TERNARY CAUSE	The network is down.
TERNARY ACTION	Check the network.

Note MAINTENANCE 112 through MAINTENANCE 117 are not used.

MAINTENANCE (118)

To troubleshoot and correct the cause of the alarm, refer to the "Domain Name Server Zone Database does not Match Between the Primary Domain Name Server and the Internal Secondary Authoritative Domain Name Server - Maintenance (118)" section on page 7-105.

DESCRIPTION	Domain Name Server Zone Database does not Match Between the Primary Domain Name Server and the Internal Secondary Authoritative Domain Name Server (DNS Zone Database does not Match Between the Primary DNS and the ISADS)
SEVERITY	CRITICAL
THRESHOLD	100
THROTTLE	0
DATAWORDS	Zone Name-STRING [64] Primary DNS Server IP-STRING [64] Serial Number of that Zone in Sl-EIGHT_BYTES Serial Number of that Zone in Ma-EIGHT_BYTES
PRIMARY CAUSE	The zone transfer between the primary DNS and the secondary DNS has failed.
PRIMARY ACTION	Check the system log monitor for the DNS traffic through port 53 (default port for DNS).

MAINTENANCE (119)

To troubleshoot and correct the cause of the alarm, refer to the "Periodic Shared Memory Database Backup Failure - Maintenance (119)" section on page 7-105.

DESCRIPTION	Periodic Shared Memory Database Backup Failure
SEVERITY	CRITICAL
THRESHOLD	100
THROTTLE	0
DATAWORDS	Reason - STRING [300] Available Disk Space (MB) - FOUR_BYTES Required Disk Space (MB) - FOUR_BYTES
PRIMARY CAUSE	High disk usage.
PRIMARY ACTION	Check disk usage.

MAINTENANCE (120)

For additional information, refer to the "Periodic Shared Memory Database Backup Success - Maintenance (120)" section on page 7-85.

DESCRIPTION	Periodic Shared Memory Database Backup Success
SEVERITY	INFO
THRESHOLD	100
THROTTLE	0
DATAWORDS	Details - STRING [300]
PRIMARY CAUSE	Successful backup of the shared memory database.
PRIMARY ACTION	The alert is informational and no further action is necessary.

Note MAINTENANCE 121 is not used.

MAINTENANCE (122)

For additional information, refer to the "Northbound Provisioning Message is Retransmitted - Maintenance (122)" section on page 85.

DESCRIPTION	Northbound Provisioning Message is Retransmitted
SEVERITY	INFO
THRESHOLD	100
THROTTLE	0
DATAWORDS	Prov Time at Seconds-FOUR_BYTES Prov Time at Milli Seconds-FOUR_BYTES Table Name-STRING [40] Update String-STRING [256]
PRIMARY CAUSE	The EMS hub maybe responding slowly.
PRIMARY ACTION	Check to see if there are any hub alarms. Take the appropriate action according to the alarms.

MAINTENANCE (123)

To monitor and correct the cause of the event, refer to the "Northbound Provisioning Message Dropped Due To Full Index Table - Maintenance (123)" section on page 85.

DESCRIPTION	Northbound Provisioning Message Dropped Due To Full Index Table
SEVERITY	WARNING
THRESHOLD	100
THROTTLE	0
DATAWORDS	Prov Time at Seconds-FOUR_BYTES Prov Time at Milli Seconds-FOUR_BYTES Table Name-STRING [40] Update String-STRING [256]
PRIMARY CAUSE	The EMS hub is not responding.
PRIMARY ACTION	Verify if there are any alarms originating from the hub and take the appropriate action.

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)	Test Report - Maintenance (1)	INFO
MAINTENANCE(2)	Report Threshold Exceeded - Maintenance (2)	INFO
MAINTENANCE(3)	Local Side has Become Faulty - Maintenance (3)	MAJOR
MAINTENANCE(4)	Mate Side has Become Faulty - Maintenance (4)	MAJOR
MAINTENANCE(5)	Changeover Failure - Maintenance (5)	MAJOR
MAINTENANCE(6)	Changeover Timeout - Maintenance (6)	MAJOR
MAINTENANCE(7)	Mate Rejected Changeover - Maintenance (7)	MAJOR
MAINTENANCE(8)	Mate Changeover Timeout - Maintenance (8)	MAJOR
MAINTENANCE(9)	Local Initialization Failure - Maintenance (9)	MAJOR
MAINTENANCE(10)	Local Initialization Timeout - Maintenance (10)	MAJOR
MAINTENANCE(11)	Switchover Complete - Maintenance (11)	INFO
MAINTENANCE(12)	Initialization Successful - Maintenance (12)	INFO
MAINTENANCE(13)	Administrative State Change - Maintenance (13)	INFO
MAINTENANCE(14)	Call Agent Administrative State Change - Maintenance (14)	INFO
MAINTENANCE(15)	Feature Server Administrative State Change - Maintenance (15)	INFO
MAINTENANCE(16)	Process Manager: Starting Process - Maintenance (16)	INFO
MAINTENANCE(17)	Invalid Event Report Received - Maintenance (17)	INFO
MAINTENANCE(18)	Process Manager: Process has Died - Maintenance (18)	MINOR
MAINTENANCE(19)	Process Manager: Process Exceeded Restart Rate - Maintenance (19)	MAJOR
MAINTENANCE(20)	Lost Connection to Mate - Maintenance (20)	MAJOR
MAINTENANCE(21)	Network Interface Down - Maintenance (21)	MAJOR
MAINTENANCE(22)	Mate is Alive - Maintenance (22)	INFO
MAINTENANCE(23)	Process Manager: Process Failed to Complete Initialization - Maintenance (23)	MAJOR
MAINTENANCE(24)	Process Manager: Restarting Process - Maintenance (24)	MINOR
MAINTENANCE(25)	Process Manager: Changing State - Maintenance (25)	INFO
MAINTENANCE(26)	Process Manager: Going Faulty - Maintenance (26)	MAJOR
MAINTENANCE(27)	Process Manager: Changing Over to Active - Maintenance (27)	INFO
MAINTENANCE(28)	Process Manager: Changing Over to Standby - Maintenance (28)	INFO
MAINTENANCE(29)	Administrative State Change Failure - Maintenance (29)	WARNING
MAINTENANCE(30)	Element Manager State Change - Maintenance (30)	INFO
MAINTENANCE(32)	Process Manager: Sending Go Active to Process - Maintenance (32)	INFO
MAINTENANCE(33)	Process Manager: Sending Go Standby to Process - Maintenance (33)	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(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
MAINTENANCE(99)	Inter-Process Communication Input Queue Depth at 50% of its Hi-Watermark - Maintenance (99)	MAJOR

Table 7-2 Cisco BTS 10200 Softswitch Maintenance Events (continued)

Event Type	Event Name	Event Severity
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
MAINTENANCE(102)	Thread Watchdog Counter Close to Expiry for a Thread - Maintenance (102)	CRITICAL
MAINTENANCE(103)	Central Processing Unit is Offline - Maintenance (103)	CRITICAL
MAINTENANCE(104)	Aggregration Device Address Successfully Resolved - Maintenance (104)	INFO
MAINTENANCE(105)	Unprovisioned Aggregration Device Detected - Maintenance (105)	WARNING
MAINTENANCE(106)	Aggregration Device Address Resolution Failure - Maintenance (106)	WARNING
MAINTENANCE(107)	No Heartbeat Messages Received Through Interface From Router - Maintenance (107)	CRITICAL
MAINTENANCE(108)	A Log File Cannot be Transferred - Maintenance (108)	WARNING
MAINTENANCE(109)	Five Successive Log Files Cannot be Transferred - Maintenance (109)	MAJOR
MAINTENANCE(110)	Access to Log Archive Facility Configuration File Failed or File Corrupted - Maintenance (110)	MAJOR
MAINTENANCE(111)	Cannot Login to External Archive Server - Maintenance (111)	CRITICAL
MAINTENANCE(118)	Domain Name Server Zone Database does not Match Between the Primary Domain Name Server and the Internal Secondary Authoritative Domain Name Server - Maintenance (118)	CRITICAL
MAINTENANCE(119)	Periodic Shared Memory Database Backup Failure - Maintenance (119)	CRITICAL
MAINTENANCE(120)	Periodic Shared Memory Database Backup Success - Maintenance (120)	INFO
MAINTENANCE(122)	Northbound Provisioning Message is Retransmitted - Maintenance (122)	INFO
MAINTENANCE(123)	Northbound Provisioning Message Dropped Due To Full Index Table - Maintenance (123)	WARNING

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 7-88.

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 7-88.

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 7-89.

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 7-89.

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 7-89.

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 7-92.

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 7-92.

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 7-92.

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 Documentation and Submitting a Service Request" section on page liii 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 7-92.

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 7-92.

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 7-93.

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 7-93.

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 7-93.

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 7-93.

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 7-93.

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 7-94.

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 7-94.

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 7-94.

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 7-94.

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 7-94.

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 7-95.

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 7-96.

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 7-96.

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 7-96.

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 7-96.

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 7-96.

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 7-97.

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 7-97.

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 Documentation and Submitting a Service Request" section on page liii 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 7-97.

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 7-97.

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 7-98.

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 7-98.

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 7-98.

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 7-98.

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 7-98.

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 7-99.

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 7-99.

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 7-99.

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 7-99.

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 7-99.

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 7-100.

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 7-100.

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 7-100.

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 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 7-100.

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 7-100.

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 7-101.

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 7-101.

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 7-101.

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 7-101.

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 7-101.

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 7-101.

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 7-102.

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 7-102.

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 7-102.

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 7-102.

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 7-102.

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 7-102.

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 7-103.

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 7-103.

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 7-104.

Aggregation Device Address Successfully Resolved - Maintenance (104)

The Aggregation Device Address Successfully Resolved event functions as an informational alert that the aggregation device address has been successfully resolved. The event is informational and no further actions is required.

Unprovisioned Aggregation Device Detected - Maintenance (105)

The Unprovisioned Aggregation Device Detected event serves as a warning that an unprovisioned aggregation device has been detected. The primary cause of the event is that the AGGR IP address is not provisioned in AGGR table. To correct the cause of the event, provision the AGGR with the AGGR IP address in the AGGR table.

Aggregation Device Address Resolution Failure - Maintenance (106)

The Aggregation Device Address Resolution Failure event serves as a warning the aggregation device address resolution has failed. The primary cause of the event is that the auto AGGR-ID resolution for the MGW IP failed due to DNS lookup failure. To correct the cause of the event, check the provisioning of DNS reverse lookup entry for the MGW IP address.

No Heartbeat Messages Received Through Interface From Router - Maintenance (107)

The No Heartbeat Messages Received Through Interface From Router alarm (critical) indicates the no HB messages are being received through the interface from the router. To troubleshoot and correct the cause of the No Heartbeat Messages Received Through Interface From Router alarm, refer to the "No Heartbeat Messages Received Through Interface From Router - Maintenance (107)" section on page 7-104.

A Log File Cannot be Transferred - Maintenance (108)

The A Log File Cannot be Transferred event serves as a warning that a log file cannot be transferred. The primary cause of the event is that there is an access problem with the external archive system. To correct the primary cause of the event, check the external archive system. The secondary cause of the event is that the network is having a problem. To correct the secondary cause of the event, check the network. The ternary cause of the event is that the source log is not present. To correct ternary cause of the event, check for the presence of a log file.

Five Successive Log Files Cannot be Transferred - Maintenance (109)

The Five Successive Log Files Cannot be Transferred alarm (major) indicates that five successive log files cannot be transferred to the archive system. To troubleshoot and correct the cause of the Five Successive Log Files Cannot be Transferred alarm, refer to the "Five Successive Log Files Cannot be Transferred - Maintenance (109)" section on page 7-104.

Access to Log Archive Facility Configuration File Failed or File Corrupted - Maintenance (110)

The Access to Log Archive Facility Configuration File Failed or File Corrupted alarm (major) indicates that access to the LAF configuration file failed or the file is corrupted. To troubleshoot and correct the cause of the Access to Log Archive Facility Configuration File Failed or File Corrupted alarm, refer to the "Access to Log Archive Facility Configuration File Failed or File Corrupted - Maintenance (110)" section on page 7-104.

Cannot Login to External Archive Server - Maintenance (111)

The Cannot Login to External Archive Server alarm (critical) indicates that the user cannot login to the external archive server. To troubleshoot and correct the cause of the Cannot Login to External Archive Server alarm, refer to the "Cannot Login to External Archive Server - Maintenance (111)" section on page 7-104.

Domain Name Server Zone Database does not Match Between the Primary Domain Name Server and the Internal Secondary Authoritative Domain Name Server - Maintenance (118)

The Domain Name Server Zone Database does not Match Between the Primary Domain Name Server and the Internal Secondary Authoritative Domain Name Server alarm (critical) indicates that the zone transfer between primary DNS and secondary DNS failed. To troubleshoot and correct the cause of the Domain Name Server Zone Database does not Match Between the Primary Domain Name Server and the Internal Secondary Authoritative Domain Name Server alarm, refer to the "Domain Name Server Zone Database does not Match Between the Primary Domain Name Server and the Internal Secondary Authoritative Domain Name Server - Maintenance (118)" section on page 7-105.

Periodic Shared Memory Database Backup Failure - Maintenance (119)

The Periodic Shared Memory Database Backup Failure alarm (critical) indicates that the periodic shared memory database backup has failed. To troubleshoot and correct the cause of the Periodic Shared Memory Database Backup Failure alarm, refer to the "Periodic Shared Memory Database Backup Failure - Maintenance (119)" section on page 7-105.

Periodic Shared Memory Database Backup Success - Maintenance (120)

The Periodic Shared Memory Database Backup Success event functions as an informational alert that the periodic shared memory database backup has been successfully completed. The event is informational and no further action is required.

Northbound Provisioning Message is Retransmitted - Maintenance (122)

The Northbound Provisioning Message is Retransmitted event serves as an informational alert that a northbound message has been retransmitted. The primary cause of the event is that EMS hub maybe responding slowly. To correct the primary cause of the event, check to see if there are any hub alarms. Take the appropriate action according to the alarms.

Northbound Provisioning Message Dropped Due To Full Index Table - Maintenance (123)

The Northbound Provisioning Message Dropped Due To Full Index Table event serves as a warning that a northbound provisioning message has been dropped due to a full index table. The primary cause of the event is that EMS hub is not responding. To correct the primary cause of the event, verify if there are any alarms originating from the hub and take the appropriate action.

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)	Local Side has Become Faulty - Maintenance (3)	MAJOR
MAINTENANCE(4)	Mate Side has Become Faulty - Maintenance (4)	MAJOR
MAINTENANCE(5)	Changeover Failure - Maintenance (5)	MAJOR
MAINTENANCE(6)	Changeover Timeout - Maintenance (6)	MAJOR
MAINTENANCE(7)	Mate Rejected Changeover - Maintenance (7)	MAJOR
MAINTENANCE(8)	Mate Changeover Timeout - Maintenance (8)	MAJOR
MAINTENANCE(9)	Local Initialization Failure - Maintenance (9)	MAJOR
MAINTENANCE(10)	Local Initialization Timeout - Maintenance (10)	MAJOR
MAINTENANCE(18)	Process Manager: Process has Died - Maintenance (18)	MINOR
MAINTENANCE(19)	Process Manager: Process Exceeded Restart Rate - Maintenance (19)	MAJOR
MAINTENANCE(20)	Lost Connection to Mate - Maintenance (20)	MAJOR
MAINTENANCE(21)	Network Interface Down - Maintenance (21)	MAJOR
MAINTENANCE(23)	Process Manager: Process Failed to Complete Initialization - Maintenance (23)	MAJOR
MAINTENANCE(24)	Process Manager: Restarting Process - Maintenance (24)	MINOR
MAINTENANCE(26)	Process Manager: Going Faulty - Maintenance (26)	MAJOR
MAINTENANCE(40)	Process Manager: Binary Does not Exist for Process - Maintenance (40)	CRITICAL
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(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(53)	The Central Processing Unit Usage is Over 90% Busy - Maintenance (53)	CRITICAL
MAINTENANCE(55)	The Five Minute Load Average is Abnormally High - Maintenance (55)	MAJOR
MAINTENANCE(57)	Memory and Swap are Consumed at Critical Levels - Maintenance (57)	CRITICAL
MAINTENANCE(61)	No Heartbeat Messages Received Through the Interface - Maintenance (61)	CRITICAL
MAINTENANCE(62)	Link Monitor: Interface Lost Communication - Maintenance (62)	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)	Thread Watchdog Counter Close to Expiry for a Thread - Maintenance (102)	CRITICAL
MAINTENANCE(103)	Central Processing Unit is Offline - Maintenance (103)	CRITICAL
MAINTENANCE(107)	No Heartbeat Messages Received Through Interface From Router - Maintenance (107)	CRITICAL
MAINTENANCE(109)	Five Successive Log Files Cannot be Transferred - Maintenance (109)	MAJOR
MAINTENANCE(110)	Access to Log Archive Facility Configuration File Failed or File Corrupted - Maintenance (110)	MAJOR
MAINTENANCE(111)	Cannot Login to External Archive Server - Maintenance (111)	CRITICAL
MAINTENANCE(118)	Domain Name Server Zone Database does not Match Between the Primary Domain Name Server and the Internal Secondary Authoritative Domain Name Server - Maintenance (118)	CRITICAL
MAINTENANCE(119)	Periodic Shared Memory Database Backup Failure - Maintenance (119)	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 Documentation and Submitting a Service Request" section on page liii 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 Documentation and Submitting a Service Request" section on page liii 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 Documentation and Submitting a Service Request" section on page liii 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 7-88. 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 Documentation and Submitting a Service Request" section on page liii 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

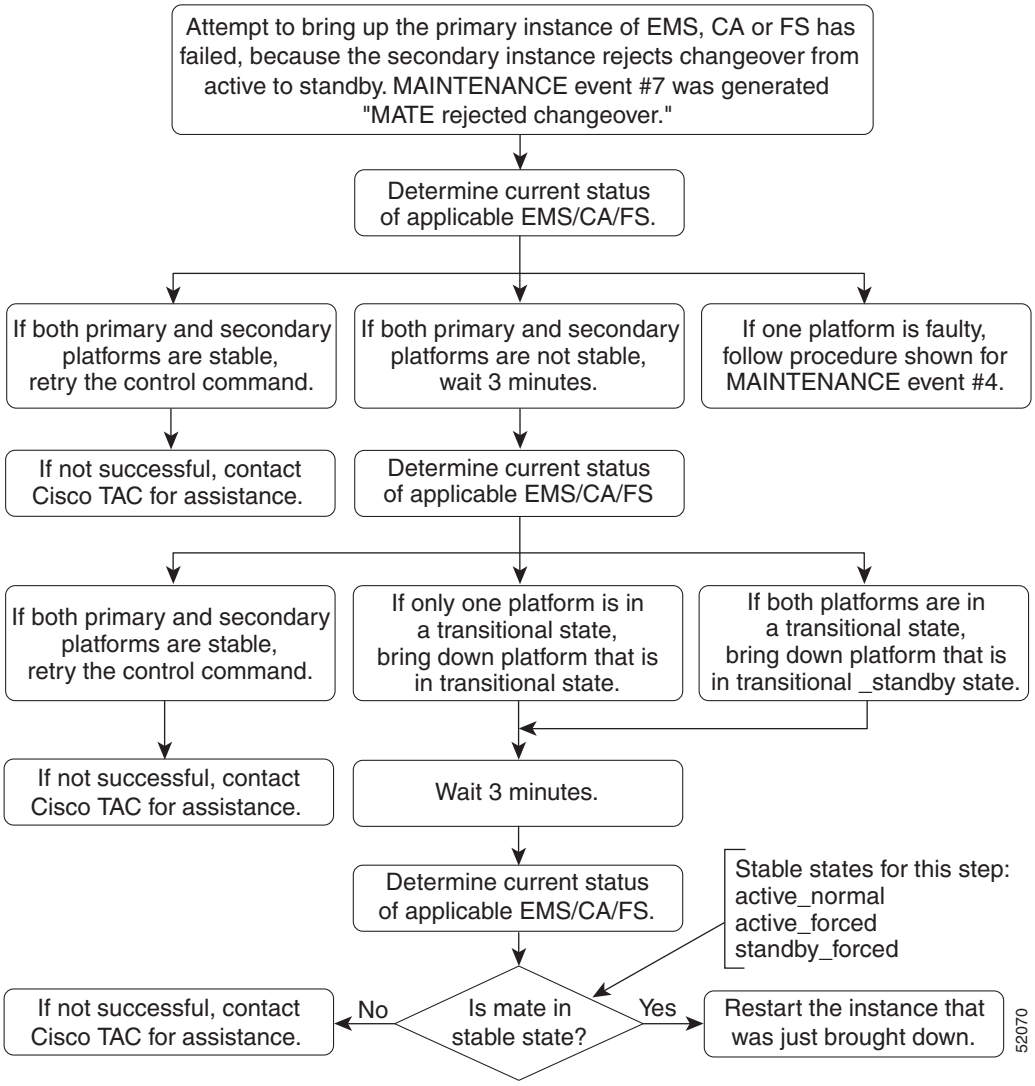
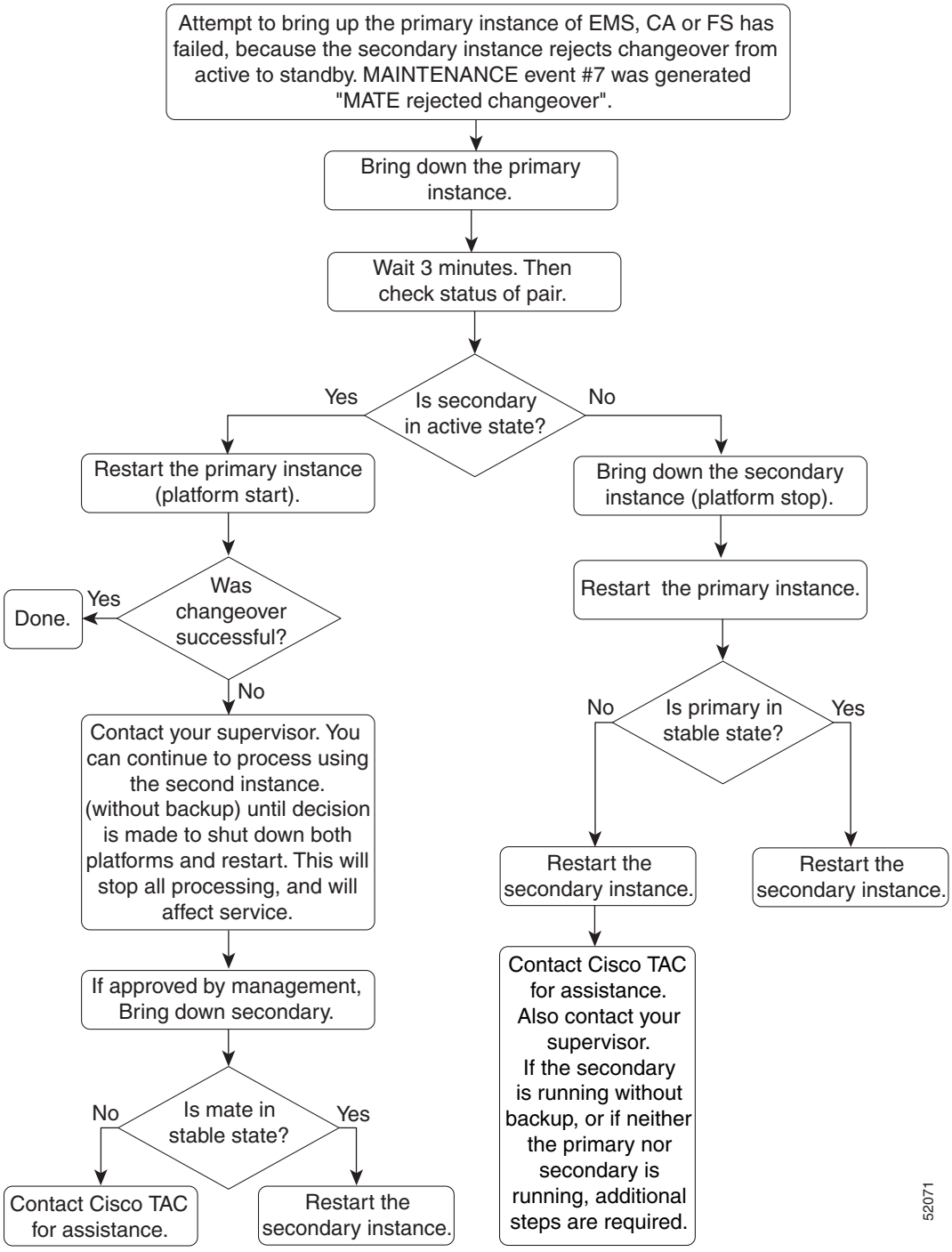


Figure 7-2 Corrective Action for Maintenance Event (7) (Mate Rejected Changeover) Primary Failed To Come Up in Active State



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 Documentation and Submitting a Service Request" section on page liii 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 Documentation and Submitting a Service Request" section on page liii 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 7-88.

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 Documentation and Submitting a Service Request" section on page liii 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 Documentation and Submitting a Service Request" section on page liii 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 Documentation and Submitting a Service Request" section on page liii 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 Documentation and Submitting a Service Request" section on page liii 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 Documentation and Submitting a Service Request" section on page liii 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 Documentation and Submitting a Service Request" section on page liii 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 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 to numerous to determine. Try to isolate the problem and Call Cisco TAC for assistance. Refer to the "Obtaining Documentation and Submitting a Service Request" section on page liii 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 Documentation and Submitting a Service Request" section on page liii 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 Documentation and Submitting a Service Request" section on page liii 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 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 ternary 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 Documentation and Submitting a Service Request" section on page liii 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 Documentation and Submitting a Service Request" section on page liii 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 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 Documentation and Submitting a Service Request" section on page liii 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 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 Documentation and Submitting a Service Request" section on page liii 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 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 Documentation and Submitting a Service Request" section on page liii 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 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 Documentation and Submitting a Service Request" section on page liii 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 an 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 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.

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 Documentation and Submitting a Service Request" section on page liii 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 Documentation and Submitting a Service Request" section on page liii 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 Documentation and Submitting a Service Request" section on page liii 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 Documentation and Submitting a Service Request" section on page liii 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 Documentation and Submitting a Service Request" section on page liii 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 Documentation and Submitting a Service Request" section on page liii 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 Documentation and Submitting a Service Request" section on page liii 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 Documentation and Submitting a Service Request" section on page liii for detailed instructions on contacting Cisco TAC and opening a service request.

No Heartbeat Messages Received Through Interface From Router - Maintenance (107)

The No Heartbeat Messages Received Through Interface From Router alarm (critical) indicates the no HB messages are being received through the interface from the router. The primary cause of the alarm is that the router is down. To correct the primary cause of alarm, restore router functionality. The secondary cause of the alarm is that the connection to the router is down. To correct the secondary cause of the alarm, restore the connection to the router. The ternary cause of the alarm is network congestion.

Five Successive Log Files Cannot be Transferred - Maintenance (109)

The Five Successive Log Files Cannot be Transferred alarm (major) indicates that five successive log files cannot be transferred to the archive system. The primary cause of the alarm is that there is a problem in access to external archive system. To correct the primary cause of the alarm, check the external archive system. The secondary cause of the alarm is that the network to external archive system is down. To correct the secondary cause of the alarm, check the status of the network.

Access to Log Archive Facility Configuration File Failed or File Corrupted - Maintenance (110)

The Access to Log Archive Facility Configuration File Failed or File Corrupted alarm (major) indicates that access to the LAF configuration file failed or the file is corrupted. The primary cause of the alarm is the LAF file is corrupted. To correct the primary cause of the alarm, check the LAF configuration file. The secondary cause of the alarm is that the LAF file is missing. To correct the secondary cause of the alarm, check for the presence of LAF configuration file.

Cannot Login to External Archive Server - Maintenance (111)

The Cannot Login to External Archive Server alarm (critical) indicates that the user cannot login to the external archive server. The primary cause of the alarm is that no authorization access is set up in external archive server for that user from Cisco BTS 10200 Softswitch. To correct the primary cause of the alarm, set up the authorization. The secondary cause of the alarm is that the external archive server is down. To correct the secondary cause of the alarm, ping the external archive server, and try to bring it up. The ternary cause of the alarm is that the network is down. To correct the ternary cause of the alarm, check the network.

Domain Name Server Zone Database does not Match Between the Primary Domain Name Server and the Internal Secondary Authoritative Domain Name Server - Maintenance (118)

The Domain Name Server Zone Database does not Match Between the Primary Domain Name Server and the Internal Secondary Authoritative Domain Name Server alarm (critical) indicates that the zone transfer between primary DNS and secondary DNS failed. To troubleshoot and correct the cause of the Domain Name Server Zone Database does not Match Between the Primary Domain Name Server and the Internal Secondary Authoritative Domain Name Server alarm, check the system log and monitor the DNS traffic through port 53 (default port for DNS).

Periodic Shared Memory Database Backup Failure - Maintenance (119)

The Periodic Shared Memory Database Backup Failure alarm (critical) indicates that the periodic shared memory database backup has failed. The primary cause of the alarm is that disk usage is high. To correct the primary cause of the alarm, check disk usage.

CHAPTER 8

Operations Support System Troubleshooting

Revised: July 22, 2009, OL-8000-32

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
	OSS (2)	OSS (5)	OSS (7)	OSS (1)
	OSS (3)	OSS (8)	OSS (9)	
	OSS (4)		OSS (11)	
	OSS (6)			
	OSS (10)			

OSS (1)

For additional information, refer to the "Test Report - Operations Support System (1)" section on page 8-8.

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 8-11.

DESCRIPTION	Undefined Variable in Known Set
SEVERITY	MAJOR
THRESHOLD	100
THROTTLE	0
DATAWORDS	Module Name - STRING [40] Field Name - STRING [40] 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 Documentation and Submitting a Service Request" section on page liii 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 8-11.

DESCRIPTION	Undefined Data Column Identification
SEVERITY	MAJOR
THRESHOLD	100
THROTTLE	0
DATAWORDS	Noun - STRING [40] 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 Documentation and Submitting a Service Request" section on page liii 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 8-11.

DESCRIPTION	Request Handler Instantiation Error
SEVERITY	MAJOR
THRESHOLD	100
THROTTLE	0
DATAWORDS	User Name - STRING [40] Host - STRING [40] Subsystem - STRING [64]
PRIMARY CAUSE	Resource limitation has prevented the creation of this object. This may come from a lack of memory or class path problem.
PRIMARY ACTION	Contact Cisco TAC for support.

Refer to the "Obtaining Documentation and Submitting a Service Request" section on page liii 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 8-12.

DESCRIPTION	Structured Query Language 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 Documentation and Submitting a Service Request" section on page liii 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 8-12.

DESCRIPTION	Structured Query Language 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 Documentation and Submitting a Service Request" section on page liii 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 8-9.

DESCRIPTION	Simple Network Management Protocol 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 Documentation and Submitting a Service Request" section on page liii 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 8-12.

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 Documentation and Submitting a Service Request" section on page liii 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 8-12.

DESCRIPTION	Simple Network Management Protocol 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 8-10.

DESCRIPTION	Queue Processing Module Database Management Index Failed with Error
SEVERITY	MAJOR
THRESHOLD	50
THROTTLE	0
DATAWORDS	Transaction ID - STRING [32] Sequence Number - EIGHT_BYTES Location Of Error - STRING [16] 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 Documentation and Submitting a Service Request" section on page liii 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 8-10.

DESCRIPTION	Queue Processing Module Database Management Index Mismatch During Add or Delete
SEVERITY	WARNING
THRESHOLD	100
THROTTLE	0
DATAWORDS	Transaction ID - STRING [32] Sequence Number - EIGHT_BYTES Location Of Error - STRING [16] 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)	Test Report - Operations Support System (1)	INFO
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(7)	Simple Network Management Protocol File Read Error - Operations Support System (7)	WARNING
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
OSS(11)	Queue Processing Module Database Management Index Mismatch During Add or Delete - Operations Support System (11)	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 8-11.

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 8-11.

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 8-11.

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 8-12.

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 8-12.

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 Documentation and Submitting a Service Request" section on page liii 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 8-12.

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 8-12.

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 8-13.

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 Documentation and Submitting a Service Request" section on page liii 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 Documentation and Submitting a Service Request" section on page liii 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 Documentation and Submitting a Service Request" section on page liii 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 Documentation and Submitting a Service Request" section on page liii 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 Documentation and Submitting a Service Request" section on page liii 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 Documentation and Submitting a Service Request" section on page liii 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 Documentation and Submitting a Service Request" section on page liii for detailed instructions on contacting Cisco TAC and opening a service request.

CHAPTER 9

Security Troubleshooting

Revised: July 22, 2009, OL-8000-32

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
	SECURITY (3)		SECURITY (2)	SECURITY (1)
			SECURITY (4)	
			SECURITY (5)	
			SECURITY (6)	

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
SEVERITY	WARNING
THRESHOLD	100
THROTTLE	0
DATAWORDS	Authentication User Name - STRING [33] From AOR - STRING [65] SIP Request Type - STRING [15] 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 9-6.

DESCRIPTION	Internet Protocol Security 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. 2. Reboot. 3. If problem persists, call the Technical Assistance Center (TAC). (Contact Cisco TAC.)

Refer to the "Obtaining Documentation and Submitting a Service Request" section on page liii 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
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
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.

SECURITY (6)

To monitor and correct the cause of the event, refer to the "Secure Session Initiation Protocol Endpoint Validation Failure - Security (6)" section on page 9-6.

DESCRIPTION	Secure Session Initiation Protocol Endpoint Validation Failure
SEVERITY	WARNING
THRESHOLD	100
THROTTLE	0
DATAWORDS	AOR - STRING [65] Secure Fqdn - STRING [65] Source IP Address - STRING [16] Violation Description - STRING [80]
PRIMARY CAUSE	Erroneous provisioning in Cisco BTS 10200 Softswitch.
PRIMARY ACTION	Check if correct value of Secure-Fqdn is provisioned in Cisco BTS 10200 Softswitch.
SECONDARY CAUSE	Erroneous provisioning in domain name system (DNS).
SECONDARY ACTION	Verify resolution of Secure-Fqdn in DNS.
TERNARY CAUSE	Erroneous provisioning in customer premises equipment (CPE).
TERNARY ACTION	Verify CPE provisioning to ensure correct source Internet Protocol (IP)/contact is used.

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)	Test Report - Security (1)	INFO
SECURITY(2)	Invalid Credentials Presented by a Session Initiation Protocol Phone - Security (2)	WARNING
SECURITY(3)	Internet Protocol Security Connection Down - Security (3)	MAJOR
SECURITY(4)	Internet Protocol Security Media Terminal Adapter Key Establish Error - Security (4)	WARNING
SECURITY(5)	Internet Protocol Security Outgoing Security Association Not Found - Security (5)	WARNING
SECURITY(6)	Secure Session Initiation Protocol Endpoint Validation Failure - Security (6)	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 9-6.

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.

Secure Session Initiation Protocol Endpoint Validation Failure - Security (6)

The Secure Session Initiation Protocol Endpoint Validation Failure event serves as a warning that a secure SIP endpoint validation failed. The primary cause of the event is that the Cisco BTS 10200 Softswitch is incorrectly provisioned. To correct the primary cause of the event, check if correct value of **secure-fqdn** is provisioned in the Cisco BTS 10200 Softswitch system. The secondary cause of the event is that the DNS is incorrectly provisioned. To correct the secondary cause of the event, verify resolution of **secure-fqdn** in the DNS. The ternary cause of the event is that the CPE is incorrectly provisioned. To correct the ternary cause of the event, verify the CPE provisioning to ensure that the correct source IP/contact being used.

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)	Internet Protocol Security Connection Down - Security (3)	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 Documentation and Submitting a Service Request" section on page liii for detailed instructions on contacting Cisco TAC and opening a service request.

CHAPTER 10

Signaling Troubleshooting

Revised: July 22, 2009, OL-8000-32

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
SIGNALING (12)	SIGNALING (7)	SIGNALING (10)	SIGNALING (4)	SIGNALING (1)
SIGNALING (64)	SIGNALING (8)	SIGNALING (14)	SIGNALING (6)	SIGNALING (42)
SIGNALING (65)	SIGNALING (9)	SIGNALING (15)	SIGNALING (25)	SIGNALING (43)
SIGNALING (69)	SIGNALING (11)	SIGNALING (16)	SIGNALING (26)	SIGNALING (44)
SIGNALING (75)	SIGNALING (13)	SIGNALING (17)	SIGNALING (27)	SIGNALING (45)
SIGNALING (80)	SIGNALING (23)	SIGNALING (18)	SIGNALING (28)	SIGNALING (46)
SIGNALING (81)	SIGNALING (59)	SIGNALING (19)	SIGNALING (29)	SIGNALING (49)
SIGNALING (82)	SIGNALING (63)	SIGNALING (20)	SIGNALING (30)	SIGNALING (50)
SIGNALING (83)	SIGNALING (66)	SIGNALING (21)	SIGNALING (31)	SIGNALING (51)
SIGNALING (84)	SIGNALING (68)	SIGNALING (22)	SIGNALING (32)	SIGNALING (52)
SIGNALING (107)	SIGNALING (79)	SIGNALING (24)	SIGNALING (33)	SIGNALING (53)
SIGNALING (110)	SIGNALING (85)	SIGNALING (36)	SIGNALING (34)	SIGNALING (54)
SIGNALING (119)	SIGNALING (86)	SIGNALING (40)	SIGNALING (60)	SIGNALING (55)
SIGNALING (120)	SIGNALING (87)	SIGNALING (78)	SIGNALING (70)	SIGNALING (57)
SIGNALING (142)	SIGNALING (88)	SIGNALING (92)	SIGNALING (71)	SIGNALING (58)
SIGNALING (144)	SIGNALING (89)	SIGNALING (93)	SIGNALING (72)	SIGNALING (61)
	SIGNALING (90)	SIGNALING (94)	SIGNALING (73)	SIGNALING (62)
	SIGNALING (91)	SIGNALING (95)	SIGNALING (74)	SIGNALING (76)
	SIGNALING (108)	SIGNALING (96)	SIGNALING (115)	SIGNALING (77)
	SIGNALING (109)	SIGNALING (97)	SIGNALING (132)	SIGNALING (104)
	SIGNALING (113)	SIGNALING (98)	SIGNALING (141)	SIGNALING (105)
	SIGNALING (114)	SIGNALING (99)	SIGNALING (146)	SIGNALING (133)
	SIGNALING (116)	SIGNALING (100)	SIGNALING (147)	SIGNALING (134)
	SIGNALING (121)	SIGNALING (101)	SIGNALING (148)	SIGNALING (135)
	SIGNALING (122)	SIGNALING (102)	SIGNALING (166)	SIGNALING (136)
	SIGNALING (125)	SIGNALING (103)	SIGNALING (167)	SIGNALING (137)
	SIGNALING (126)	SIGNALING (106)		SIGNALING (139)
	SIGNALING (127)	SIGNALING (111)		SIGNALING (140)
		SIGNALING (112)		SIGNALING (152)

Table 10-1 Signaling Events and Alarms by Severity (continued)

CRITICAL	MAJOR	MINOR	WARNING	INFO
		SIGNALING (117)		
		SIGNALING (118)		
		SIGNALING (124)		
		SIGNALING (138)		
		SIGNALING (143)		
		SIGNALING (145)		
		SIGNALING (150)		
		SIGNALING (151)		

SIGNALING (1)

For additional information, refer to the "Test Report - Signaling (1)" section on page 10-82.

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

Note SIGNALING (2) and SIGNALING (3) are not used.

SIGNALING (4)

To monitor and correct the cause of the event, refer to the "Invalid Message Received - Signaling (4)" section on page 10-82.

DESCRIPTION	Invalid Message Received
SEVERITY	WARNING
THRESHOLD	100
THROTTLE	0
DATAWORDS	Endpoint Name - STRING [40] 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 10-82.

DESCRIPTION	Database Module Function Call Failure
SEVERITY	WARNING
THRESHOLD	100
THROTTLE	0
DATAWORDS	Endpoint Name - STRING [40] Return Code - FOUR_BYTES Function Name - STRING [64] Calling Function - STRING [64] 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 10-111.

DESCRIPTION	Socket Failure
SEVERITY	MAJOR
THRESHOLD	30
THROTTLE	0
DATAWORDS	Reason Text - STRING [30]
PRIMARY CAUSE	Issued when there is a failure in creating/binding to the User Datagram Protocol (UDP) socket.
PRIMARY ACTION	Verify there is no conflict in port assignment with other processes in the system and ensure no previous instance of the same process is still running.
SECONDARY CAUSE	Software logic problem.
SECONDARY ACTION	Contact Cisco Support. (Contact Cisco Technical Assistance Center (TAC).)

Refer to the "Obtaining Documentation and Submitting a Service Request" section on page liii for detailed instructions on contacting Cisco TAC and opening a service request.

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 10-111.

DESCRIPTION	Session Initiation Protocol 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 Documentation and Submitting a Service Request" section on page liii 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 10-112.

DESCRIPTION	Timeout on Internet Protocol Address
SEVERITY	MAJOR
THRESHOLD	100
THROTTLE	0
DATAWORDS	MGW/Term Name - STRING [80] Gateway Type - STRING [32] Possible Cause - STRING [32]
PRIMARY CAUSE	Issued when opticall 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 10-112.

DESCRIPTION	Failed to Send Complete Session Initiation Protocol 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.

Refer to the "Obtaining Documentation and Submitting a Service Request" section on page liii 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 10-112.

DESCRIPTION	Failed to Allocate Session Initiation Protocol Control Block
SEVERITY	MAJOR
THRESHOLD	100
THROTTLE	0
DATAWORDS	Size - TWO_BYTES 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 10-113.

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] 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 10-114.

DESCRIPTION	Signaling System 7 Signaling Link Down
SEVERITY	MAJOR
THRESHOLD	100
THROTTLE	0
DATAWORDS	Link_Number - ONE_BYTE 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 10-115.

DESCRIPTION	Link is Remotely Inhibited
SEVERITY	MINOR
THRESHOLD	100
THROTTLE	0
DATAWORDS	Link - ONE_BYTE 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 10-115.

DESCRIPTION	Link is Locally Inhibited
SEVERITY	MINOR
THRESHOLD	100
THROTTLE	0
DATAWORDS	Link No - ONE_BYTE 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 10-115.

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 10-115.

DESCRIPTION	Link: Local Processor Outage
SEVERITY	MINOR
THRESHOLD	100
THROTTLE	0
DATAWORDS	Link No - ONE_BYTE 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 10-115.

DESCRIPTION	Link: Remote Processor Outage
SEVERITY	MINOR
THRESHOLD	100
THROTTLE	0
DATAWORDS	Link No - ONE_BYTE 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 10-115.

DESCRIPTION	Link Set Inaccessible
SEVERITY	MAJOR
THRESHOLD	100
THROTTLE	0
DATAWORDS	Link Set No - ONE_BYTE 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 10-116.

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.

SIGNALING (21)

To troubleshoot and correct the cause of the alarm, refer to the "Route Set Failure - Signaling (21)" section on page 10-116.

DESCRIPTION	Route Set Failure
SEVERITY	MAJOR
THRESHOLD	200
THROTTLE	0
DATAWORDS	Route Set No - TWO_BYTES 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 10-116.

DESCRIPTION	Route Set Congested
SEVERITY	MINOR
THRESHOLD	100
THROTTLE	0
DATAWORDS	Route Set No - TWO_BYTES Route Set Name - STRING [8] 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 10-117.

DESCRIPTION	Destination Point Code 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: 1) A failure in the affected DPC. 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 10-118.

DESCRIPTION	Destination Point Code Congested
SEVERITY	MINOR
THRESHOLD	100
THROTTLE	0
DATAWORDS	DPC - STRING [12] DPC Type - ONE_BYTE 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 - Signaling (25)" section on page 10-85.

DESCRIPTION	Unanswered Blocking
SEVERITY	WARNING
THRESHOLD	100
THROTTLE	0
DATAWORDS	CIC Number - TWO_BYTES TGN-ID - FOUR_BYTES DPC - STRING [20] OPC - STRING [20]
PRIMARY CAUSE	Issued when a blocking (BLO) message was not acknowledged before the timer 13 (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 10-85.

DESCRIPTION	Unanswered Unblocking Message
SEVERITY	WARNING
THRESHOLD	100
THROTTLE	0
DATAWORDS	CIC Number - TWO_BYTES TGN-ID - FOUR_BYTES DPC - STRING [20] 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 - Signaling (27)" section on page 10-86.

DESCRIPTION	Unanswered Circuit Group Blocking
SEVERITY	WARNING
THRESHOLD	100
THROTTLE	0
DATAWORDS	CIC Number - TWO_BYTES TGN-ID - FOUR_BYTES DPC - STRING [20] 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 - Signaling (28)" section on page 10-86.

DESCRIPTION	Unanswered Circuit Group Unblocking
SEVERITY	WARNING
THRESHOLD	100
THROTTLE	0
DATAWORDS	CIC Number - TWO_BYTES TGN-ID - FOUR_BYTES DPC - STRING [20] 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 10-86.

DESCRIPTION	Unanswered Circuit Query Message
SEVERITY	WARNING
THRESHOLD	100
THROTTLE	0
DATAWORDS	CIC Number - TWO_BYTES TGN-ID - FOUR_BYTES DPC - STRING [20] 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 - Signaling (30)" section on page 10-86.

DESCRIPTION	Unanswered Circuit Validation Test
SEVERITY	WARNING
THRESHOLD	100
THROTTLE	0
DATAWORDS	CIC Number - TWO_BYTES TGN-ID - FOUR_BYTES DPC - STRING [20] 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 - Signaling (31)" section on page 10-86.

DESCRIPTION	Unanswered Reset Circuit
SEVERITY	WARNING
THRESHOLD	100
THROTTLE	0
DATAWORDS	CIC Number - TWO_BYTES TGN-ID - FOUR_BYTES DPC - STRING [20] 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 - Signaling (32)" section on page 10-87.

DESCRIPTION	Unanswered Group Reset
SEVERITY	WARNING
THRESHOLD	100
THROTTLE	0
DATAWORDS	CIC Number - TWO_BYTES TGN-ID - FOUR_BYTES DPC - STRING [20] 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 - Signaling (33)" section on page 10-87.

DESCRIPTION	Unanswered Release
SEVERITY	WARNING
THRESHOLD	100
THROTTLE	0
DATAWORDS	CIC Number - TWO_BYTES TGN-ID - FOUR_BYTES DPC - STRING [20] 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 - Signaling (34)" section on page 10-87.

DESCRIPTION	Unanswered Continuity Check Request
SEVERITY	WARNING
THRESHOLD	100
THROTTLE	0
DATAWORDS	CIC Number - TWO_BYTES TGN-ID - FOUR_BYTES DPC - STRING [20] OPC - STRING [20]
PRIMARY CAUSE	Issued when an loop prevention acknowledgement (LPA) message was not acknowledged before the timer continuity check request (T_{CCR}) 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 10-118. For add it on al information on correcting the cause of the alarm, refer to Appendix B, "System Usage of MGW Keepalive Parameters, Release 4.5.x."

DESCRIPTION	Trunk Locally Blocked
SEVERITY	MINOR
THRESHOLD	500
THROTTLE	0
DATAWORDS	CIC Number - STRING [40] TGN-ID - FOUR_BYTES DPC - STRING [20] OPC - STRING [20] MGW-EP-NAME - STRING [64] MGW-TSAP-ADDR - STRING [80] Reason - STRING [80]
PRIMARY CAUSE	Issued when a BLO or CGB message was sent on the specified CIC.
PRIMARY ACTION	For add it on al information on correcting the cause of the alarm, refer to Appendix B, "System Usage of MGW Keepalive Parameters, Release 4.5.x."

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 10-118.

DESCRIPTION	Trunk Remotely Blocked
SEVERITY	MAJOR
THRESHOLD	500
THROTTLE	0
DATAWORDS	CIC Number - STRING [40] TGN-ID - FOUR_BYTES DPC - STRING [20] OPC - STRING [20] MGW-EP-NAME - STRING [64] 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 SERVICE OOS message is received for Integrated Services Digital Network (ISDN) trunks. Issued when Reverse Make Busy (rbz) signal 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 10-88.

DESCRIPTION	Continuity Testing Message Received on the Specified Circuit Identification Code
SEVERITY	INFO
THRESHOLD	100
THROTTLE	0
DATAWORDS	CIC Number - TWO_BYTES TGN-ID - FOUR_BYTES DPC - STRING [20] 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 10-88.

DESCRIPTION	Release Complete Received in Response to Reset Circuit Message on the Specified Circuit Identification Code
SEVERITY	INFO
THRESHOLD	100
THROTTLE	0
DATAWORDS	CIC Number - TWO_BYTES TGN-ID - FOUR_BYTES DPC - STRING [20] 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 10-88.

DESCRIPTION	Continuity Recheck is Performed on Specified Circuit Identification Code
SEVERITY	INFO
THRESHOLD	100
THROTTLE	0
DATAWORDS	CIC Number - TWO_BYTES TGN-ID - FOUR_BYTES DPC - STRING [20] 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 10-88.

DESCRIPTION	Circuit is UNEQUIPPED on Remote Side
SEVERITY	INFO
THRESHOLD	100
THROTTLE	0
DATAWORDS	CIC Number - TWO_BYTES TGN-ID - FOUR_BYTES DPC - STRING [20] 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 10-88.

DESCRIPTION	Specified Circuit Identification Code is Invalid for the Operation
SEVERITY	INFO
THRESHOLD	100
THROTTLE	0
DATAWORDS	CIC Number - TWO_BYTES TGN-ID - FOUR_BYTES DPC - STRING [20] 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 10-88.

DESCRIPTION	A General Processing Error Encountered
SEVERITY	INFO
THRESHOLD	100
THROTTLE	0
DATAWORDS	CIC Number - TWO_BYTES TGN-ID - FOUR_BYTES DPC - STRING [20] 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 10-89.

DESCRIPTION	Unexpected Message for the Call State is Received: Clear Call
SEVERITY	INFO
THRESHOLD	100
THROTTLE	0
DATAWORDS	CIC Number - TWO_BYTES TGN-ID - FOUR_BYTES DPC - STRING [20] 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 10-89.

DESCRIPTION	Set Trunk State as Remotely Unequipped
SEVERITY	INFO
THRESHOLD	100
THROTTLE	0
DATAWORDS	CIC Number - TWO_BYTES TGN-ID - FOUR_BYTES DPC - STRING [20] 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 10-89.

DESCRIPTION	Set Trunk State as NOT Remotely Blocked
SEVERITY	INFO
THRESHOLD	100
THROTTLE	0
DATAWORDS	CIC Number - TWO_BYTES TGN-ID - FOUR_BYTES DPC - STRING [20] 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 10-89.

DESCRIPTION	Set Trunk State as Remotely Blocked
SEVERITY	INFO
THRESHOLD	100
THROTTLE	0
DATAWORDS	CIC Number - TWO_BYTES TGN-ID - FOUR_BYTES DPC - STRING [20] 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 10-89.

DESCRIPTION	Circuit Validation Test Aborted
SEVERITY	INFO
THRESHOLD	100
THROTTLE	0
DATAWORDS	CIC Number - TWO_BYTES TGN-ID - FOUR_BYTES DPC - STRING [20] 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 10-89.

DESCRIPTION	Circuit Validation Successful
SEVERITY	INFO
THRESHOLD	100
THROTTLE	0
DATAWORDS	CIC Number - TWO_BYTES TGN-ID - FOUR_BYTES DPC - STRING [20] 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 10-90.

DESCRIPTION	Continuity Recheck Failed
SEVERITY	INFO
THRESHOLD	100
THROTTLE	0
DATAWORDS	CIC Number - TWO_BYTES TGN-ID - FOUR_BYTES DPC - STRING [20] 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 10-90.

DESCRIPTION	Continuity Recheck Successful
SEVERITY	INFO
THRESHOLD	100
THROTTLE	0
DATAWORDS	CIC Number - TWO_BYTES TGN-ID - FOUR_BYTES DPC - STRING [20] 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 10-118.

DESCRIPTION	Auto State Change for Integrated Services Digital Network Trunk Group by Media Gateway
SEVERITY	MAJOR
THRESHOLD	100
THROTTLE	0
DATAWORDS	Trunk Group ID - FOUR_BYTES Trunk Group Index - FOUR_BYTES Media Gateway Name - STRING [65] Media Gateway Index - FOUR_BYTES 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 10-90.

DESCRIPTION	Integrated Services Digital Network STATUS Message Containing Error Indication Received
SEVERITY	WARNING
THRESHOLD	100
THROTTLE	0
DATAWORDS	Termination Name - STRING [40] Termination Index - FOUR_BYTES Trunk Group ID - FOUR_BYTES Trunk Group Index - FOUR_BYTES Cause Value - ONE_BYTE 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 10-90.

DESCRIPTION	Trunk Operational State Changed by Service Message
SEVERITY	INFO
THRESHOLD	100
THROTTLE	0
DATAWORDS	Termination Name - STRING [40] Termination Index - FOUR_BYTES Trunk Group ID - FOUR_BYTES Trunk Group Index - FOUR_BYTES 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 10-91.

DESCRIPTION	Received Integrated Services Digital Network RESTART Message
SEVERITY	INFO
THRESHOLD	100
THROTTLE	0
DATAWORDS	Termination Name - STRING [40] Termination Index - FOUR_BYTES Trunk Group ID - FOUR_BYTES Trunk Group Index - FOUR_BYTES 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 10-119.

DESCRIPTION	Media Gateway/Termination Faulty
SEVERITY	MAJOR
THRESHOLD	100
THROTTLE	0
DATAWORDS	Fully Qualified Name - STRING [80] Type of Gateway - STRING [32] 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 10-119.

DESCRIPTION	Media Gateway Adapter 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 Documentation and Submitting a Service Request" section on page liii 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 10-119.

DESCRIPTION	Media Gateway Adapter 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 Documentation and Submitting a Service Request" section on page liii 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 10-119.

DESCRIPTION	Call Agent Internal Error (Because of Which Media Gateway Adapter has to Start Automatically)
SEVERITY	MAJOR
THRESHOLD	100
THROTTLE	0
DATAWORDS	Fully Qualified Name - STRING [80] Reason - STRING [80] 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 Documentation and Submitting a Service Request" section on page liii 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 Endpoints are out of Service at Gateway - Signaling (68)" section on page 10-119.

DESCRIPTION	Media Gateway Endpoints are out of Service at Gateway
SEVERITY	MAJOR
THRESHOLD	100
THROTTLE	0
DATAWORDS	Fully Qualified Name - STRING [80] Type of MGW- STRING [32] Failure Cause - STRING [80] Subscriber Info - STRING [80] ICMP Ping Status - STRING [80]
PRIMARY CAUSE	This could have been caused by (1) The media gateway has been administratively taken OOS using command in gateway (GW). (2) The endpoint is alarmed/OOS state.
PRIMARY ACTION	Bring the Media gateway has been administratively taken INS using command in GW. Fix the endpoint alarms.

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 10-120.

DESCRIPTION	Call Agent and Feature Server 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 10-92.

DESCRIPTION	Integrated Services Digital Network Unable to Restore D-channel Due to Failed Communication
SEVERITY	WARNING
THRESHOLD	100
THROTTLE	0
DATAWORDS	Trunk Group ID - FOUR_BYTES 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 10-92.

DESCRIPTION	Integrated Services Digital Network Unable to Establish D-channel
SEVERITY	WARNING
THRESHOLD	100
THROTTLE	0
DATAWORDS	Trunk Group ID - FOUR_BYTES Trunk Group Index - FOUR_BYTES
PRIMARY CAUSE	The 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.
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 10-92.

DESCRIPTION	Integrated Services Digital Network - Calls Lost Due to D-channel Down for Period of Time
SEVERITY	WARNING
THRESHOLD	100
THROTTLE	0
DATAWORDS	Trunk Group ID - FOUR_BYTES 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 10-93.

DESCRIPTION	Integrated Services Digital Network - Unable to Send RESTART Due to RESTART Timer Expired
SEVERITY	WARNING
THRESHOLD	100
THROTTLE	0
DATAWORDS	Termination Name - STRING [40] Termination Index - FOUR_BYTES Trunk Group ID - FOUR_BYTES Trunk Group Index - FOUR_BYTES 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 10-93.

DESCRIPTION	Integrated Services Digital Network: Unable to Send the SERVICE Due to the SERVICE Timer Expired
SEVERITY	WARNING
THRESHOLD	100
THROTTLE	0
DATAWORDS	Termination Name - STRING [40] Termination Index - FOUR_BYTES Trunk Group ID - FOUR_BYTES Trunk Group Index - FOUR_BYTES 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 10-120.

DESCRIPTION	Signaling System 7 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 "**start -i omni**" to bring up SS7 stack.

SIGNALING (76)

For additional information, refer to the "Timeout on Remote Instance - Signaling (76)" section on page 10-93.

DESCRIPTION	Timeout on Remote Instance
SEVERITY	INFO
THRESHOLD	100
THROTTLE	0
DATAWORDS	Port Number - TWO_BYTES 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 10-93.

DESCRIPTION	Integrated Services Digital Network D-channel Switchover for Non-Facility Associated Signaling
SEVERITY	INFO
THRESHOLD	100
THROTTLE	0
DATAWORDS	Trunk Group ID - FOUR_BYTES 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 10-120.

DESCRIPTION	Integrated Services Digital Network Single D-channel Down for Non-Facility Associated Signaling
SEVERITY	MINOR
THRESHOLD	100
THROTTLE	0
DATAWORDS	Trunk Group ID - FOUR_BYTES Trunk Group Idx - FOUR_BYTES 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 10-120. For add it on al information on correcting the cause of the alarm, refer to Appendix B, "System Usage of MGW Keepalive Parameters, Release 4.5.x."

DESCRIPTION	Media Gateway Unreachable
SEVERITY	MAJOR
THRESHOLD	100
THROTTLE	0
DATAWORDS	Entity Name - STRING [40] General Context - STRING [40] Specific Context - STRING [40] Failure Context - STRING [40]
PRIMARY CAUSE	MGCP signaling interop error has occurred.
PRIMARY ACTION	Notify customer support or refer to Appendix B, "System Usage of MGW Keepalive Parameters, Release 4.5.x". (Contact Cisco TAC.)

Refer to the "Obtaining Documentation and Submitting a Service Request" section on page liii 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 10-120.

DESCRIPTION	Out of Bounds, Memory/Socket Error
SEVERITY	CRITICAL
DATAWORDS	Process Name - STRING [40] Description - STRING [40] 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 Documentation and Submitting a Service Request" section on page liii 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 10-121.

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 Documentation and Submitting a Service Request" section on page liii 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 10-121.

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 Documentation and Submitting a Service Request" section on page liii 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 10-121.

DESCRIPTION	Error While Binding to Socket
SEVERITY	CRITICAL
THRESHOLD	100
THROTTLE	0
DATAWORDS	Gateway ID - STRING [32] Socket ID - FOUR_BYTES Local TSAP Address - STRING [32] Reason - STRING [128]

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 10-121.

DESCRIPTION	Reached Maximum Socket Limit
SEVERITY	CRITICAL
THRESHOLD	100
THROTTLE	0
DATAWORDS	Gateway ID - STRING [32] 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 10-121.

DESCRIPTION	Initialization Failure
SEVERITY	CRITICAL
THRESHOLD	100
THROTTLE	0
DATAWORDS	Gateway ID - STRING [32] 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 10-121.

DESCRIPTION	Remote H323 Gateway is not Reachable
SEVERITY	MAJOR
THRESHOLD	100
THROTTLE	0
DATAWORDS	Gateway ID - STRING [32] 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 10-122.

DESCRIPTION	H323 Message Parsing Error
SEVERITY	MAJOR
THRESHOLD	100
THROTTLE	0
DATAWORDS	Gateway ID - STRING [32] 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 Documentation and Submitting a Service Request" section on page liii 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 10-122.

DESCRIPTION	H323 Message Encoding Error
SEVERITY	MAJOR
THRESHOLD	100
THROTTLE	0
DATAWORDS	Gateway ID - STRING [32] 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 Documentation and Submitting a Service Request" section on page liii 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 10-122.

DESCRIPTION	Gatekeeper not Available/Reachable
SEVERITY	MAJOR
THRESHOLD	100
THROTTLE	0
DATAWORDS	Gateway ID - STRING [32] Gatekeeper ID - STRING [32] 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. 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 its content or call Cisco TAC. (Contact Cisco TAC.)

Refer to the "Obtaining Documentation and Submitting a Service Request" section on page liii for detailed instructions on contacting Cisco TAC and opening a service request.

SIGNALING (90)

To troubleshoot and correct the cause of the alarm, refer to the "Alternate Gatekeeper is not Responding - Signaling (90)" section on page 10-122.

DESCRIPTION	Alternate Gatekeeper is not Responding
SEVERITY	MAJOR
THRESHOLD	100
THROTTLE	0
DATAWORDS	Gateway ID - STRING [32] Gatekeeper ID - STRING [32] 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. 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 its content or call Cisco TAC. (Contact Cisco TAC.)

Refer to the "Obtaining Documentation and Submitting a Service Request" section on page liii for detailed instructions on contacting Cisco TAC and opening a service request.

SIGNALING (91)

To troubleshoot and correct the cause of the alarm, refer to the "Endpoint Security Violation - Signaling (91) (H.323)" section on page 10-123.

DESCRIPTION	Endpoint Security Violation
SEVERITY	MAJOR
THRESHOLD	100
THROTTLE	0
DATAWORDS	Gateway ID - STRING [32] Gatekeeper ID - STRING [32] 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 10-123.

DESCRIPTION	Invalid Call Identifier
SEVERITY	MINOR
THRESHOLD	100
THROTTLE	0
DATAWORDS	Gateway ID - STRING [32] Remote GW TSAP Addr - STRING [32] 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 Documentation and Submitting a Service Request" section on page liii 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 10-123.

DESCRIPTION	Invalid Call Reference Value
SEVERITY	MINOR
THRESHOLD	100
THROTTLE	0
DATAWORDS	Gateway ID - STRING [32] Remote GW TSAP Addr - STRING [32] Call ID - EIGHT_BYTES 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 Documentation and Submitting a Service Request" section on page liii 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 10-123.

DESCRIPTION	Invalid Conference Identifier
SEVERITY	MINOR
THRESHOLD	100
THROTTLE	0
DATAWORDS	Gateway ID - STRING [32] Reason - STRING [32] Remote GW Port - TWO_BYTES Call ID - EIGHT_BYTES 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 Documentation and Submitting a Service Request" section on page liii 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 10-123.

DESCRIPTION	Invalid Message from the Network
SEVERITY	MINOR
THRESHOLD	100
THROTTLE	0
DATAWORDS	Gateway ID - STRING [32] Remote GW TSAP Addr - STRING [32] Call ID - EIGHT_BYTES Conf ID - EIGHT_BYTES 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 Documentation and Submitting a Service Request" section on page liii 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 10-124.

DESCRIPTION	Internal Call Processing Error
SEVERITY	MINOR
THRESHOLD	100
THROTTLE	0
DATAWORDS	Gateway ID - STRING [32] Call ID - EIGHT_BYTES Reason - STRING [128]
PRIMARY CAUSE	A software error has occurred.
PRIMARY ACTION	Call Cisco TAC. (Contact Cisco TAC.)

Refer to the "Obtaining Documentation and Submitting a Service Request" section on page liii 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 10-124.

DESCRIPTION	Insufficient Information to Complete Call
SEVERITY	MINOR
THRESHOLD	100
THROTTLE	0
DATAWORDS	Gateway ID - STRING [32] Call ID - EIGHT_BYTES Conf ID - EIGHT_BYTES 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 Documentation and Submitting a Service Request" section on page liii 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 10-124.

DESCRIPTION	H323 Protocol Inconsistencies
SEVERITY	MINOR
THRESHOLD	100
THROTTLE	0
DATAWORDS	Gateway ID - STRING [32] Call ID - EIGHT_BYTES 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 Documentation and Submitting a Service Request" section on page liii 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 10-124.

DESCRIPTION	Abnormal Call Clearing
SEVERITY	MINOR
THRESHOLD	100
THROTTLE	0
DATAWORDS	Gateway ID - STRING [32] Call ID - EIGHT_BYTES 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 Documentation and Submitting a Service Request" section on page liii 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 10-124.

DESCRIPTION	Codec Negotiation Failed
SEVERITY	MINOR
THRESHOLD	100
THROTTLE	0
DATAWORDS	Gateway ID - STRING [32] Call ID - EIGHT_BYTES 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 10-124.

DESCRIPTION	Per Call Security Violation
SEVERITY	MINOR
THRESHOLD	100
THROTTLE	0
DATAWORDS	Gateway ID - STRING [32] Call ID - EIGHT_BYTES 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 10-125.

DESCRIPTION	H323 Network Congested
SEVERITY	MINOR
THRESHOLD	100
THROTTLE	0
DATAWORDS	Gateway ID - STRING [32] 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 10-125.

DESCRIPTION	Aggregation 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 10-97.

DESCRIPTION	Aggregation 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 10-98.

DESCRIPTION	Aggregation Gate Set Failed
SEVERITY	INFO
THRESHOLD	100
THROTTLE	0
DATAWORDS	AGGR-ID - STRING [16] Error-Code - TWO_BYTES Sub-Error-Code - TWO_BYTES
PRIMARY CAUSE	Gate set acknowledgement never came from 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 10-125.

DESCRIPTION	Enhanced Subscriber Authentication Cisco BTS 10200 Softswitch Delivery Function 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 10-125.

DESCRIPTION	Logical Internet Protocol Addresses not Mapped Correctly
SEVERITY	CRITICAL
THRESHOLD	30
THROTTLE	0
DATAWORDS	Contact Domain Name - STRING [128] Number of IP Addresses Resolved - FOUR_BYTES 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.

Refer to the "Obtaining Documentation and Submitting a Service Request" section on page liii 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 "Simplex Only Operational Mode - Signaling (108)" section on page 10-126.

DESCRIPTION	Simplex Only Operational Mode
SEVERITY	MAJOR
THRESHOLD	30
THROTTLE	0
DATAWORDS	Host Domain Name - STRING [128]
PRIMARY CAUSE	The hostname parameter specified in platform.cfg file instead of -contact parameter.
PRIMARY ACTION	Cisco BTS 10200 Softswitch is configured as a SIMPLEX system.
SECONDARY CAUSE	SIP adapter (SIA) host and contact parameters are the same in the platform.cfg file. SIA is configured for use on a simplex system.
SECONDARY ACTION	If this is a duplex installation, regardless of current operational state, contact Cisco TAC. If this is a simplex installation only, this alarm can be turned off.

Refer to the "Obtaining Documentation and Submitting a Service Request" section on page liii 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 10-126.

DESCRIPTION	Stream Control Transmission Protocol 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 10-130.

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 10-130.

DESCRIPTION	Stream Control Transmission Protocol Association Degraded (One of Two Internet Protocol Connections Down)
SEVERITY	MAJOR
THRESHOLD	100
THROTTLE	0
DATAWORDS	SCTP Association ID - STRING [17] 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 10-130.

DESCRIPTION	Stream Control Transmission Protocol 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 10-131.

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 10-131.

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 snooper 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 10-100.

DESCRIPTION	Invalid Routing Context Received
SEVERITY	WARNING
THRESHOLD	100
THROTTLE	0
DATAWORDS	Invalid Routing Cont - FOUR_BYTES 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 10-132.

DESCRIPTION	Destination Point Code 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 10-132.

DESCRIPTION	Circuit Validation Test Message Received for an Unequipped Circuit Identification Code
SEVERITY	MINOR
THRESHOLD	100
THROTTLE	0
DATAWORDS	CIC - TWO_BYTES TGN-ID - EIGHT_BYTES 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 10-132.

DESCRIPTION	Circuit Verification Response Received with Failed Indication
SEVERITY	MINOR
THRESHOLD	100
THROTTLE	0
DATAWORDS	CIC - TWO_BYTES TGN-ID - EIGHT_BYTES DPC - STRING [20] 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 10-132.

DESCRIPTION	Signaling System 7 Adapter 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 10-132.

DESCRIPTION	Signaling System 7 Module/Signaling System 7 Adapter 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 10-133.

DESCRIPTION	Message Transfer Part 3 User Adapter 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 10-133.

DESCRIPTION	Message Transfer Part 3 User Adapter 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 10-133.

DESCRIPTION	Remote Subsystem is Out Of Service
SEVERITY	MINOR
THRESHOLD	100
THROTTLE	0
DATAWORDS	Destination Point Co - STRING [20] 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 10-133.

DESCRIPTION	Signaling Connection Control Part 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 10-134.

DESCRIPTION	Signaling Connection Control Part Binding Failure
SEVERITY	MAJOR
THRESHOLD	100
THROTTLE	0
DATAWORDS	Local Point Code - STRING [20] 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 10-134.

DESCRIPTION	Transaction Capabilities Application Part 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 10-102.

DESCRIPTION	Transaction Capabilities Application Part 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 10-102.

DESCRIPTION	Unable to Decode Generic Transport Descriptor Message
SEVERITY	INFO
THRESHOLD	100
THROTTLE	0
DATAWORDS	Endpoint Name - STRING [40] 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 10-103.

DESCRIPTION	Signaling System 7 Message Encoding Failure
SEVERITY	INFO
THRESHOLD	100
THROTTLE	0
DATAWORDS	CIC Number - TWO_BYTES TGN-ID - FOUR_BYTES DPC - STRING [20] 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 Documentation and Submitting a Service Request" section on page liii 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 10-103.

DESCRIPTION	Signaling System 7 Message Decoding Failure
SEVERITY	INFO
THRESHOLD	100
THROTTLE	0
DATAWORDS	CIC Number - TWO_BYTES TGN-ID - FOUR_BYTES DPC - STRING [20] 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 Documentation and Submitting a Service Request" section on page liii 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 10-103.

DESCRIPTION	Signaling System 7 Message Invalid Received
SEVERITY	INFO
THRESHOLD	100
THROTTLE	0
DATAWORDS	CIC Number - TWO_BYTES TGN-ID - FOUR_BYTES DPC - STRING [20] 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.
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 Documentation and Submitting a Service Request" section on page liii 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 10-103.

DESCRIPTION	Signaling System 7 Confusion Message Received
SEVERITY	INFO
THRESHOLD	100
THROTTLE	0
DATAWORDS	CIC Number - TWO_BYTES TGN-ID - FOUR_BYTES DPC - STRING [20] 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. (Contact Cisco TAC.)

Refer to the "Obtaining Documentation and Submitting a Service Request" section on page liii for detailed instructions on contacting Cisco TAC and opening a service request.

SIGNALING (138)

To monitor and correct the cause of the event, refer to the "Number of Open Session Initiation Protocol Connections is Reaching Engineered Limit - Signaling (138)" section on page 10-103.

DESCRIPTION	Number of Open Session Initiation Protocol Connections is Reaching Engineered Limit
SEVERITY	WARNING
THRESHOLD	100
THROTTLE	0
DATAWORDS	Number of SIP Connections Open - FOUR_BYTES SIP Connection Alarm Threshold - FOUR_BYTES Open SIP Connection Limit - FOUR_BYTES
PRIMARY CAUSE	Call failure/feature unavailable.
PRIMARY ACTION	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. Please contact Cisco support. (Contact Cisco TAC.)

Refer to the "Obtaining Documentation and Submitting a Service Request" section on page liii 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 10-104.

DESCRIPTION	Signaling System 7 Trunk was Found to be in Erroneous State
SEVERITY	INFO
THRESHOLD	100
THROTTLE	0
DATAWORDS	CIC - TWO_BYTES TGN-ID - FOUR_BYTES DPC - STRING [20] OPC - STRING [20] Near-End State - STRING [64] Far-End State - STRING [64] 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 10-104.

DESCRIPTION	Unanswered Information Message
SEVERITY	INFO
THRESHOLD	100
THROTTLE	0
DATAWORDS	CIC - TWO_BYTES TGN-ID - FOUR_BYTES DPC - STRING [20] 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 10-104.

DESCRIPTION	Address not Resolved by Domain Name System 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 10-134.

DESCRIPTION	Session Initiation Protocol Trunk Operationally Out-of-Service
SEVERITY	CRITICAL
THRESHOLD	100
THROTTLE	0
DATAWORDS	Trunk Group Description - STRING [16] 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 10-134.

DESCRIPTION	Internet Protocol Interface Link to the Signaling System 7 Signaling Gateway is Down
SEVERITY	MINOR
THRESHOLD	100
THROTTLE	0
DATAWORDS	Interface Name - STRING [65] 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 10-134.

DESCRIPTION	All Internet Protocol Interface Links to Signaling System 7 Signaling Gateway are Down
SEVERITY	CRITICAL
THRESHOLD	100
THROTTLE	0
DATAWORDS	Interface Name - STRING [65] 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 10-135.

DESCRIPTION	One Internet Protocol Interface to Signaling System 7 Signaling Gateway is Down
SEVERITY	MINOR
THRESHOLD	100
THROTTLE	0
DATAWORDS	Interface Name - STRING [65] Interface IP Address - STRING [65]
PRIMARY CAUSE	Hardware problem has occurred.
PRIMARY ACTION	Check the link interfaces.

SIGNALING (146)

To monitor and correct the cause of the event, refer to the "All Retransmission Attempts of Session Initiation Protocol Request or Response Failed - Signaling (146)" section on page 10-105.

DESCRIPTION	All Retransmission Attempts of Session Initiation Protocol Request or Response Failed
SEVERITY	WARNING
THRESHOLD	100
THROTTLE	0
DATAWORDS	SIP Request Type - STRING [15] Sender IP - STRING [20]
PRIMARY CAUSE	SIP request: All retransmission attempts for a SIP request failed for DNS or IP address of request uniform resource identifier (URI). SIP response: All retransmission attempts for a SIP response failed for received socket IP address of request and DNS (or IP address) of via header.
PRIMARY ACTION	Ensure if DNS server is up and running for host name resolution and provisioned properly to resolve to correct order of IP addresses. Ensure that previous hop network component is alive and in healthy state for failures related to SIP responses.

SIGNALING (147)

To monitor and correct the cause of the event, refer to the "Domain Name System Service Addresses Exhausted - Signaling (147)" section on page 10-105.

DESCRIPTION	Domain Name System Service Addresses Exhausted
SEVERITY	WARNING
THRESHOLD	100
THROTTLE	0
DATAWORDS	SRV Hostname - STRING [256]
PRIMARY CAUSE	DNS service (SRV) hostname resolution to IP address exhausted.
PRIMARY ACTION	Add entry to SRV in DNS server. Fix Cisco BTS 10200 Softswitch provisioning.

SIGNALING (148)

To monitor and correct the cause of the event, refer to the "Softswitch Audit Released Stale Memory - Signaling (148)" section on page 10-106.

DESCRIPTION	Softswitch Audit Released Stale Memory
SEVERITY	WARNING
THRESHOLD	100
THROTTLE	0
DATAWORDS	Stale Memory Release Info - STRING [128]
PRIMARY CAUSE	Loss of communication with originating or terminating side.
PRIMARY ACTION	Check if adjacent network element is up and having proper communication link with the BTS 10200 Softswitch.
SECONDARY CAUSE	Adjacent network device protocol error.
SECONDARY ACTION	Check the adjacent network device protocol compatibility.
TERNARY CAUSE	An internal software error has occurred.
TERNARY ACTION	Contact BTS 10200 engineer. (Contact Cisco TAC.)

Refer to the "Obtaining Documentation and Submitting a Service Request" section on page liii for detailed instructions on contacting Cisco TAC and opening a service request.

Note SIGNALING (149) is 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 10-135.

DESCRIPTION	Stream Control Transmission Protocol Association Congested
SEVERITY	MINOR
THRESHOLD	100
THROTTLE	0
DATAWORDS	SCTP Association ID - STRING [17] 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.

SIGNALING (151)

To troubleshoot and correct the cause of the alarm, refer to the "Termination Permanent Error Code Received - Signaling (151)" section on page 10-135.

DESCRIPTION	Termination Permanent Error Code Received
SEVERITY	MINOR
THRESHOLD	100
THROTTLE	0
DATAWORDS	End Point /Termination - STRING [54] Media Gateway - STRING [54] MGCP Message Type - STRING [54]
PRIMARY CAUSE	Fault in the gateway device.
PRIMARY ACTION	Maintenance required on the gateway or termination.

SIGNALING (152)

For additional information, refer to the "Termination Transient Error Received - Signaling (152)" section on page 10-106.

DESCRIPTION	Termination Transient Error Received
SEVERITY	INFO
THRESHOLD	100
THROTTLE	0
DATAWORDS	Entity Name - STRING [40] General Context - STRING [40] Specific Context - STRING [40] Failure Context - STRING [40]
PRIMARY CAUSE	MGCP signaling interop errors have occurred.
PRIMARY ACTION	Notify customer support. (Contact Cisco TAC.)

Refer to the "Obtaining Documentation and Submitting a Service Request" section on page liii for detailed instructions on contacting Cisco TAC and opening a service request.

Note SIGNALING (153) through SIGNALING (165) are not used.

SIGNALING (166)

To monitor and correct the cause of the event, refer to the "No Routing Keys are Active - Signal (166)" section on page 106.

DESCRIPTION	No Routing Keys are Active
SEVERITY	WARNING
THRESHOLD	0
THROTTLE	0
PRIMARY CAUSE	Routing keys not controlled into ACTIVE state.
PRIMARY ACTION	Control routing keys to ACTIVE state.
SECONDARY CAUSE	The ITP provisioning is incorrect.
SECONDARY ACTION	Check the ITP provisioning.

SIGNALING (167)

To monitor and correct the cause of the event, refer to the "No Signaling Gateways are Active – Signaling (167)" section on page 107.

DESCRIPTION	No Signaling Gateways are Active
SEVERITY	WARNING
THRESHOLD	0
THROTTLE	0
PRIMARY CAUSE	A communication problem between ITP and the Cisco BTS 10200 Softswitch.
PRIMARY ACTION	Check the communication path between the Cisco BTS 10200 Softswitch and the ITP.

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)	Test Report - Signaling (1)	INFO
SIGNALING(4)	Invalid Message Received - Signaling (4)	WARNING
SIGNALING(6)	Database Module Function Call Failure - Signaling (6)	WARNING
SIGNALING(7)	Socket Failure - Signaling (7)	MAJOR
SIGNALING(8)	Session Initiation Protocol Message Receive Failure - Signaling (8)	MAJOR
SIGNALING(9)	Timeout on Internet Protocol Address - Signaling (9)	MAJOR
SIGNALING(10)	Failed to Send Complete Session Initiation Protocol Message - Signaling (10)	MINOR
SIGNALING(11)	Failed to Allocate Session Initiation Protocol Control Block - Signaling (11)	MAJOR
SIGNALING(12)	Feature Server is not Up or is not Responding to Call Agent - Signaling (12)	CRITICAL
SIGNALING(13)	Signaling System 7 Signaling Link Down - Signaling (13)	MAJOR
SIGNALING(14)	Link is Remotely Inhibited - Signaling (14)	MINOR
SIGNALING(15)	Link is Locally Inhibited - Signaling (15)	MINOR
SIGNALING(16)	Link is Congested - Signaling (16)	MINOR
SIGNALING(17)	Link: Local Processor Outage - Signaling (17)	MINOR
SIGNALING(18)	Link: Remote Processor Outage - Signaling (18)	MINOR
SIGNALING(19)	Link Set Inaccessible - Signaling (19)	MAJOR
SIGNALING(20)	Link Set Congestion - Signaling (20)	MAJOR
SIGNALING(21)	Route Set Failure - Signaling (21)	MAJOR
SIGNALING(22)	Route Set Congested - Signaling (22)	MINOR
SIGNALING(23)	Destination Point Code Unavailable - Signaling (23)	MAJOR
SIGNALING(24)	Destination Point Code Congested - Signaling (24)	MINOR
SIGNALING(25)	Unanswered Blocking - Signaling (25)	WARNING
SIGNALING(26)	Unanswered Unblocking Message - Signaling (26)	WARNING
SIGNALING(27)	Unanswered Circuit Group Blocking - Signaling (27)	WARNING
SIGNALING(28)	Unanswered Circuit Group Unblocking - Signaling (28)	WARNING
SIGNALING(29)	Unanswered Circuit Query Message - Signaling (29)	WARNING
SIGNALING(30)	Unanswered Circuit Validation Test - Signaling (30)	WARNING
SIGNALING(31)	Unanswered Reset Circuit - Signaling (31)	WARNING
SIGNALING(32)	Unanswered Group Reset - Signaling (32)	WARNING
SIGNALING(33)	Unanswered Release - Signaling (33)	WARNING
SIGNALING(34)	Unanswered Continuity Check Request - Signaling (34)	WARNING
SIGNALING(36)	Trunk Locally Blocked - Signaling (36)	MINOR

Table 10-2 Cisco BTS 10200 Softswitch Signaling Events (continued)

Event Type	Event Name	Event Severity
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(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(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
SIGNALING(68)	Media Gateway Endpoints are out of Service at Gateway - 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

Table 10-2 Cisco BTS 10200 Softswitch Signaling Events (continued)

Event Type	Event Name	Event Severity
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
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

Table 10-2 Cisco BTS 10200 Softswitch Signaling Events (continued)

Event Type	Event Name	Event Severity
SIGNALING(107)	Logical Internet Protocol Addresses not Mapped Correctly - Signaling (107)	CRITICAL
SIGNALING(108)	Simplex Only Operational Mode - 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(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(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

Table 10-2 Cisco BTS 10200 Softswitch Signaling Events (continued)

Event Type	Event Name	Event Severity
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)	All Retransmission Attempts of Session Initiation Protocol Request or Response Failed - Signaling (146)	WARNING
SIGNALING(147)	Domain Name System Service Addresses Exhausted - Signaling (147)	WARNING
SIGNALING(148)	Softswitch Audit Released Stale Memory - Signaling (148)	WARNING
SIGNALING(150)	Stream Control Transmission Protocol Association Congested - Signaling (150)	MINOR
SIGNALING(151)	Termination Permanent Error Code Received - Signaling (151)	MINOR
SIGNALING(152)	Termination Transient Error Received - Signaling (152)	INFO
SIGNALING(166)	No Routing Keys are Active - Signal (166)	WARNING
SIGNALING(167)	No Signaling Gateways are Active – Signaling (167)	WARNING

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.

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/binding to the UDP socket. To troubleshoot and correct the cause of the Socket Failure alarm, refer to the "Socket Failure - Signaling (7)" section on page 10-111.

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 10-111.

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 10-112.

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 10-112.

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 10-112.

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 10-113.

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 10-114.

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 10-115.

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 10-115.

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 10-115.

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 10-115.

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 10-115.

Link Set Inaccessible - Signaling (19)

The Link Set Inaccessible alarm (major) indicates that the specified SS7 link in inaccessible. To troubleshoot and correct the cause of the Link Set Inaccessible alarm, refer to the "Link Set Inaccessible - Signaling (19)" section on page 10-115.

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 10-116.

Route Set Failure - Signaling (21)

The Route Set Failure alarm (major) indicates that the specified route set has a 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 10-116.

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 10-116.

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 10-117.

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 10-118.

Unanswered Blocking - Signaling (25)

The Unanswered Blocking 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 - Signaling (27)

The Unanswered Circuit Group Blocking 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 - Signaling (28)

The Unanswered Circuit Group Unblocking 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 - Signaling (30)

The Unanswered Circuit Validation Test 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 Tcvt 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 - Signaling (31)

The Unanswered Reset Circuit 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 - Signaling (32)

The Unanswered Group Reset event serves as a warning that a GRS message was not answered. The primary cause of the event is that a 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 - Signaling (33)

The Unanswered Release 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 - Signaling (34)

The Unanswered Continuity Check Request 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_{CCR} 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 10-118. For add it on al information on correcting the cause of the alarm, refer to Appendix B, "System Usage of MGW Keepalive Parameters, Release 4.5.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 10-118.

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 in 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 a 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 even 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 at 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 10-118.

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 10-119.

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 10-119.

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 10-119.

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 10-119.

Media Gateway Endpoints are out of Service at Gateway - Signaling (68)

The Media Gateway Endpoints are out of Service at Gateway alarm (major) indicates that the media gateway endpoints are out of service at the GW. To troubleshoot and correct the cause of the Media Gateway Endpoints are out of Service at Gateway alarm, refer to the "Media Gateway Endpoints are out of Service at Gateway - Signaling (68)" section on page 10-119.

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 10-120.

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 in 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 10-120.

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 10-120.

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 10-120. For add it on al information on correcting the cause of the alarm, refer to Appendix B, "System Usage of MGW Keepalive Parameters, Release 4.5.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 10-120.

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 10-121.

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 10-121.

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 10-121.

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 10-121.

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 10-121.

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 10-121.

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 10-122.

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 10-122.

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 10-122.

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 10-122.

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 10-123.

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 10-123.

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 10-123.

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 10-123.

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 10-123.

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 10-124.

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 10-124.

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 10-124.

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 10-124.

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 10-124.

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 10-124.

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 10-125.

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 10-125.

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 10-125.

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 10-125.

Simplex Only Operational Mode - Signaling (108)

The Simplex Only Operational Mode 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 Simplex Only Operational Mode alarm, refer to the "Simplex Only Operational Mode - Signaling (108)" section on page 10-126.

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 10-126.

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 10-130.

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 10-130.

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 10-130.

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 10-131.

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 10-131.

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 10-132.

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 10-132.

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 10-132.

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 10-133.

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 10-133.

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 10-133.

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 10-133.

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 10-134.

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 10-134.

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 Documentation and Submitting a Service Request" section on page liii 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 Documentation and Submitting a Service Request" section on page liii 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 Documentation and Submitting a Service Request" section on page liii 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 Documentation and Submitting a Service Request" section on page liii 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 event functions as an informational alert that the number of open SIP connections is reaching the engineered limit. The primary cause of the event is that the call failed or a feature is not available. To correct the primary cause of the event, is to increase the engineered limit to allow for more open connections. System configuration and traffic load have caused the number of open connections to approach the

engineered limit. Contact Cisco TAC for assistance in increasing in the limit. Refer to the "Obtaining Documentation and Submitting a Service Request" section on page liii for detailed instructions on contacting Cisco TAC and opening a service request.

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 10-134.

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 10-134.

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 10-134.

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 10-135.

All Retransmission Attempts of Session Initiation Protocol Request or Response Failed - Signaling (146)

The All Retransmission Attempts of Session Initiation Protocol Request or Response Failed event serves as a warning the all retransmission attempts of a SIP request or response failed. The primary cause of the event is that all retransmission attempts for a SIP request failed for a DNS or an IP address of the request URI or all retransmission attempts for a SIP response failed for the received socket IP address of the request and the DNS (or IP address). To correct the primary cause of the event, ensure that the DNS server is up and running for host name resolution and provisioned properly to resolve to correct order of IP addresses and ensure that previous hop network component is alive and in a healthy state for failures related to SIP responses.

Domain Name System Service Addresses Exhausted - Signaling (147)

The Domain Name System Service Addresses Exhausted event serves as a warning that all DNS SRV addresses are exhausted. The primary cause of the event is that the DNS SRV hostname resolution to IP address is exhausted. To correct the primary cause of the event, add an entry to the SRV in the DNS server and fix the Cisco BTS 10200 Softswitch provisioning.

Softswitch Audit Released Stale Memory - Signaling (148)

The Softswitch Audit Released Stale Memory event serves as a warning that an audit released stale memory event has occurred. The primary cause of the event is that a loss of communication with originating or terminating side has occurred. To correct the primary cause of the event, check to see if adjacent network element is up and having proper communication link with the BTS 10200 Softswitch. The secondary cause of the event is that an adjacent network device has had a protocol error. To correct the secondary cause of the event, check the adjacent network device protocol for compatibility. The ternary cause of the event is that an internal software error has occurred. To correct the ternary cause of the event, contact Cisco TAC. Refer to the "Obtaining Documentation and Submitting a Service Request" section on page liii for detailed instructions on contacting Cisco TAC and opening a service request.

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 10-135.

Termination Permanent Error Code Received - Signaling (151)

The Termination Permanent Error Code Received alarm (minor) indicates that a termination permanent error code was received. To troubleshoot and correct the cause of the Termination Permanent Error Code Received alarm, refer to the "Termination Permanent Error Code Received - Signaling (151)" section on page 10-135.

Termination Transient Error Received - Signaling (152)

The Termination Transient Error Received event functions as an informational alert that a termination transient error was received. The primary cause of the event that the MGCP signaling process has inter-operational errors. To correct the primary cause of the event, notify Cisco TAC. Refer to the "Obtaining Documentation and Submitting a Service Request" section on page liii for detailed instructions on contacting Cisco TAC and opening a service request.

No Routing Keys are Active - Signal (166)

The No Routing Keys are Active event serves as a warning that no routing keys are active. The primary cause of the event is that the routing keys are not controlled into ACTIVE state. To correct the primary cause of the event, control the routing keys to the ACTIVE state. The secondary cause of the event is that the ITP provisioning is incorrect. To correct the secondary cause of the event, check the ITP provisioning.

No Signaling Gateways are Active – Signaling (167)

The No Signaling Gateways are Active event serves as a warning that no signaling gateways are active. The primary cause of the event is that there is a communication problem between ITP and the Cisco BTS 10200 Softswitch. To correct the primary cause of the event, check the communication path between Cisco BTS 10200 Softswitch and the ITP.

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)	Socket Failure - Signaling (7)	MAJOR
SIGNALING(8)	Session Initiation Protocol Message Receive Failure - Signaling (8)	MAJOR
SIGNALING(9)	Timeout on Internet Protocol Address - Signaling (9)	MAJOR
SIGNALING(10)	Failed to Send Complete Session Initiation Protocol Message - Signaling (10)	MINOR
SIGNALING(11)	Failed to Allocate Session Initiation Protocol Control Block - Signaling (11)	MAJOR
SIGNALING(12)	Feature Server is not Up or is not Responding to Call Agent - Signaling (12)	CRITICAL
SIGNALING(13)	Signaling System 7 Signaling Link Down - Signaling (13)	MAJOR
SIGNALING(14)	Link is Remotely Inhibited - Signaling (14)	MINOR
SIGNALING(15)	Link is Locally Inhibited - Signaling (15)	MINOR
SIGNALING(16)	Link is Congested - Signaling (16)	MINOR
SIGNALING(17)	Link: Local Processor Outage - Signaling (17)	MINOR
SIGNALING(18)	Link: Remote Processor Outage - Signaling (18)	MINOR
SIGNALING(19)	Link Set Inaccessible - Signaling (19)	MAJOR
SIGNALING(20)	Link Set Congestion - Signaling (20)	MAJOR
SIGNALING(21)	Route Set Failure - Signaling (21)	MAJOR
SIGNALING(22)	Route Set Congested - Signaling (22)	MINOR
SIGNALING(23)	Destination Point Code Unavailable - Signaling (23)	MAJOR
SIGNALING(24)	Destination Point Code Congested - Signaling (24)	MINOR
SIGNALING(36)	Trunk Locally Blocked - Signaling (36)	MINOR
SIGNALING(40)	Trunk Remotely Blocked - Signaling (40)	MAJOR
SIGNALING(59)	Auto State Change for Integrated Services Digital Network Trunk Group by Media Gateway - Signaling (59)	MAJOR
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
SIGNALING(68)	Media Gateway Endpoints are out of Service at Gateway - Signaling (68)	MAJOR
SIGNALING(69)	Call Agent and Feature Server Communication Message Timeout - Signaling (69)	CRITICAL
SIGNALING(75)	Signaling System 7 Stack not Ready - Signaling (75)	CRITICAL
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

Table 10-3 Cisco BTS 10200 Softswitch Signaling Alarms (continued)

Alarm Type	Alarm Name	Alarm Severity
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)	Simplex Only Operational Mode - 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(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(150)	Stream Control Transmission Protocol Association Congested - Signaling (150)	MINOR
SIGNALING(151)	Termination Permanent Error Code Received - Signaling (151)	MINOR

Socket Failure - Signaling (7)

The Socket Failure alarm (major) indicates that there is a failure in creating/binding to the UDP socket. The primary cause of the alarm is that there is a failure in creating or binding to the UDP socket. To correct the primary cause of the alarm, verify that there is no conflict in port assignment with other processes in the system and ensure no previous instance of the same process is still running. The secondary cause of the alarm is that a software logic problem has occurred. To correct the secondary cause of the alarm, contact Cisco TAC. Refer to the "Obtaining Documentation and Submitting a Service Request" section on page liii for detailed instructions on contacting Cisco TAC and opening a service request.

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 Documentation and Submitting a Service Request" section on page liii 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 Documentation and Submitting a Service Request" section on page liii 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.

Use the following steps to locate and correct provisioning errors which may be associated with the Feature Server is not Up or is not Responding to Call Agent alarm:

Step 1 Verify that the ID, TSAP-ADDR, and TYPE are properly provisioned in the Feature Server (feature-server) table.

Step 2 Verify that Alerting Notification is provisioned properly.

Step 3 Verify one of the following cases, as applicable:

- Verify that Alerting Notification is included in the SERVICE table applicable to the specific subscriber.
- Verify that Alerting Notification is included in the SERVICE table applicable to the specific POP (the service ID identified by the office-service-id token in the POP table).
- Verify that Alerting Notification is included in the default office service ID (if the feature is intended to be offered by default to all subscribers on the switch).

Note In the procedures included in this document, Alerting Notification 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 POP;
SHOW SERVICE ID=<the value of the office-service-id in POP table>
SHOW CA-CONFIG TYPE=DEFAULT-OFFICE-SERVICE-ID;
SHOW SERVICE ID=<the value of the default-office-service-id in ca-config table>
SHOW SERVICE ID=silverservice;
SHOW SUBSCRIBER-SERVICE-PROFILE SERVICE-ID=silverservice;
```

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 the 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.

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 ternary cause of the alarm is that the SS7 link may be disconnected or faulty. To correct the ternary 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 in 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 a 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 10-130. 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 10-133. 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 add it on al information on correcting the cause of the alarm, refer to Appendix B, “System Usage of MGW Keepalive Parameters, Release 4.5.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 Documentation and Submitting a Service Request" section on page liii 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 Documentation and Submitting a Service Request" section on page liii 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 Documentation and Submitting a Service Request" section on page liii for detailed instructions on contacting Cisco TAC and opening a service request.

Media Gateway Endpoints are out of Service at Gateway - Signaling (68)

The Media Gateway Endpoints are out of Service at Gateway alarm (major) indicates that the media gateway endpoints are out of service at the GW. The primary causes of the alarm are that the Media gateway has been administratively taken the OOS using a command in GW or the Endpoint is in an alarmed or OOS state. To correct the primary cause of the alarm, bring into service the Media gateway that has been administratively taken INS using the command in GW and fix the endpoint alarms.

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 in not ready. The primary cause of the alarm that the SS7 stack 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 B, "System Usage of MGW Keepalive Parameters, Release 4.5.x"or contact Cisco TAC. Refer to the "Obtaining Documentation and Submitting a Service Request" section on page liii for detailed instructions on contacting Cisco TAC and opening a service request. For add it on al information on correcting the cause of the alarm, refer to Appendix B, "System Usage of MGW Keepalive Parameters, Release 4.5.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. 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 Documentation and Submitting a Service Request" section on page liii 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 ternary cause of the alarm is that a socket error has occurred. An inappropriate or already bound socket may be in use. To correct the ternary 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 Documentation and Submitting a Service Request" section on page liii 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 Documentation and Submitting a Service Request" section on page liii 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.

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 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 Documentation and Submitting a Service Request" section on page liii 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 Documentation and Submitting a Service Request" section on page liii 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.

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 its content or contact Cisco TAC. Refer to the "Obtaining Documentation and Submitting a Service Request" section on page liii for detailed instructions on contacting Cisco TAC and opening a service request.

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.

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 its content or contact Cisco TAC. Refer to the "Obtaining Documentation and Submitting a Service Request" section on page liii for detailed instructions on contacting Cisco TAC and opening a service request.

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 Documentation and Submitting a Service Request" section on page liii 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 Documentation and Submitting a Service Request" section on page liii 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 Documentation and Submitting a Service Request" section on page liii 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 Documentation and Submitting a Service Request" section on page liii 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 Documentation and Submitting a Service Request" section on page liii 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 Documentation and Submitting a Service Request" section on page liii 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 Documentation and Submitting a Service Request" section on page liii 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 Documentation and Submitting a Service Request" section on page liii 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 it's 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 opticall.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 ternary cause of the alarm is that the IP address manager is not running. To correct the ternary 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 Documentation and Submitting a Service Request" section on page liii for detailed instructions on contacting Cisco TAC and opening a service request.

Simplex Only Operational Mode - Signaling (108)

The Simplex Only Operational Mode 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 -hostname parameter is specified in the platform.cfg file (instead of the -contact parameter). The Cisco BTS 10200 Softswitch is configured as a SIMPLEX system. The secondary cause of the alarm is that the SIA host and contact parameters are the same in platform.cfg file or the SIA is configured for use on a simplex system. To correct the secondary cause of the alarm, if this is a duplex installation, regardless of current operational state, contact Cisco TAC. If this is a simplex installation only, this alarm can be turned off. Refer to the "Obtaining Documentation and Submitting a Service Request" section on page liii 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.cgf | 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 -mdlgarbagetimer 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 t he 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 snooper 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 10-131 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 snooper 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 10-130, or contact the Cisco TAC for assistance in resolving this issue.

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 ternary cause of the alarm is that the IP Routing Table is not configured properly. To correct the ternary 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 10-130 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.

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 10-130 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 snooper 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 10-130. Otherwise, the problem is at the M3UA layer. Call the Cisco TAC for assistance.

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 10-130 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 10-130 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.

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.

Termination Permanent Error Code Received - Signaling (151)

The Termination Permanent Error Code Received alarm (minor) indicates that a termination permanent error code was received. The primary cause of the alarm is that a fault has occurred in the gateway device. To correct the primary cause of the alarm, maintenance required on the gateway or termination.

CHAPTER 11

Statistics Troubleshooting

Revised: July 22, 2009, OL-8000-32

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
	STATISTICS (12)		STATISTICS (8)	STATISTICS (1)
	STATISTICS (13)		STATISTICS (9)	STATISTICS (2)
			STATISTICS (10)	STATISTICS (3)
			STATISTICS (11)	STATISTICS (4)
				STATISTICS (5)
				STATISTICS (6)
				STATISTICS (7)

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
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
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
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
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] Traffic Mgr Msg Type - STRING [40] 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 Documentation and Submitting a Service Request" section on page liii 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
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 Documentation and Submitting a Service Request" section on page liii 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
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 Documentation and Submitting a Service Request" section on page liii 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
SEVERITY	WARNING
THRESHOLD	100
THROTTLE	0
DATAWORDS	Message Type - STRING [40] 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	**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.

Refer to the "Obtaining Documentation and Submitting a Service Request" section on page liii 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 Syncronization - 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
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)	Test Report - Statistics (1)	INFO
STATISTICS(2)	Call Agent Measurement Collection Started - Statistics (2)	INFO
STATISTICS(3)	Call Agent Measurement Collection Finished - Statistics (3)	INFO
STATISTICS(4)	Plain Old Telephone Service/Centrex/Telecommunications Data Link Monitor Feature Server Measurement Collection Started - Statistics (4)	INFO
STATISTICS(5)	Plain Old Telephone Service/Centrex/Telecommunications Data Link Monitor Feature Server Measurement Collection Finished - Statistics (5)	INFO
STATISTICS(6)	Advanced Intelligent Network Feature Server Measurement Collection Started - Statistics (6)	INFO
STATISTICS(7)	Advanced Intelligent Network Feature Server Measurement Collection Finished - Statistics (7)	INFO
STATISTICS(8)	Message Send Failure - Statistics (8)	WARNING
STATISTICS(9)	Measurement Table Structured Query Language Read Error - Statistics (9)	WARNING
STATISTICS(10)	Measurement Table Structured Query Language Write Error - Statistics (10)	WARNING
STATISTICS(11)	Measurement Collection Application Programming Interface Failure - Statistics (11)	WARNING
STATISTICS(12)	Measurement Handshake Error - Schema Inconsistency - Statistics (12)	MAJOR
STATISTICS(13)	Traffic and Measurements Module Application Programming Interface Failure - Statistics (13)	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 Documentation and Submitting a Service Request" section on page liii 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 Documentation and Submitting a Service Request" section on page liii 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 Documentation and Submitting a Service Request" section on page liii 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 Documentation and Submitting a Service Request" section on page liii 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)	Measurement Handshake Error - Schema Inconsistency - Statistics (12)	MAJOR
STATISTICS(13)	Traffic and Measurements Module Application Programming Interface Failure - Statistics (13)	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 ternary cause of the alarm is that the shared memory table has overflown. To correct the ternary 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: July 22, 2009, OL-8000-32

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
SYSTEM (13)	SYSTEM (8)	SYSTEM (2)	SYSTEM (5)	SYSTEM (1)
	SYSTEM (12)	SYSTEM (3)	SYSTEM (9)	
		SYSTEM (4)		
		SYSTEM (6)		
		SYSTEM (7)		
		SYSTEM (10)		
		SYSTEM (11)		
		SYSTEM (14)		

SYSTEM (1)

For additional information, refer to the "Test Report - System (1)" section on page 12-11.

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 12-14.

DESCRIPTION	Inter-Process Communication Queue Read Failure
SEVERITY	MINOR
THRESHOLD	100
THROTTLE	0
DATAWORDS	Queue Name - STRING [20] 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 Documentation and Submitting a Service Request" section on page liii 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 12-14.

DESCRIPTION	Inter-Process Communication Message Allocate Failure
SEVERITY	MINOR
THRESHOLD	100
THROTTLE	0
DATAWORDS	Requested Size - TWO_BYTES Error Code - FOUR_BYTES 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 Documentation and Submitting a Service Request" section on page liii 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 12-15.

DESCRIPTION	Inter-Process Communication Message Send Failure
SEVERITY	MINOR
THRESHOLD	50
THROTTLE	0
DATAWORDS	Error Code - FOUR_BYTES Destination Process - FOUR_BYTES Message Number - FOUR_BYTES 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 Documentation and Submitting a Service Request" section on page liii 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 12-12.

DESCRIPTION	Unexpected Inter-Process Communication Message Received
SEVERITY	WARNING
THRESHOLD	100
THROTTLE	0
DATAWORDS	Source Process Type - ONE_BYTE Source Thread Type - ONE_BYTE Message Number - TWO_BYTES 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 Documentation and Submitting a Service Request" section on page liii 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 12-15.

DESCRIPTION	Index List Insert Error
SEVERITY	MINOR
THRESHOLD	100
THROTTLE	0
DATAWORDS	List Name - STRING [20] Index of Entry Being - FOUR_BYTES 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 Documentation and Submitting a Service Request" section on page liii 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 12-15.

DESCRIPTION	Index List Remove Error
SEVERITY	MINOR
THRESHOLD	100
THROTTLE	0
DATAWORDS	List Name - STRING [20] Index of Entry Being - FOUR_BYTES 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 Documentation and Submitting a Service Request" section on page liii 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 12-15.

DESCRIPTION	Thread Creation Failure
SEVERITY	MAJOR
THRESHOLD	100
THROTTLE	0
DATAWORDS	Error Code - FOUR_BYTES Thread Name - STRING [20] 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 Documentation and Submitting a Service Request" section on page liii 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 12-12.

DESCRIPTION	Timer Start Failure
SEVERITY	WARNING
THRESHOLD	100
THROTTLE	0
DATAWORDS	Timer Type - STRING [20] 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 Documentation and Submitting a Service Request" section on page liii 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 12-15.

DESCRIPTION	Index Update Registration Error
SEVERITY	MINOR
THRESHOLD	100
THROTTLE	0
DATAWORDS	Error Code - FOUR_BYTES Table Name - STRING [20] 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 Documentation and Submitting a Service Request" section on page liii 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 12-16.

DESCRIPTION	Index Table Add Entry Error
SEVERITY	MINOR
THRESHOLD	100
THROTTLE	0
DATAWORDS	Table Name - STRING [20] Index of Entry Being - FOUR_BYTES Error Code - FOUR_BYTES 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 Documentation and Submitting a Service Request" section on page liii 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 12-16.

DESCRIPTION	Software Error
SEVERITY	MAJOR
THRESHOLD	100
THROTTLE	0
DATAWORDS	Context Description - STRING [80] FileName - STRING [20] Line Number of Code - TWO_BYTES 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 Documentation and Submitting a Service Request" section on page liii for detailed instructions on contacting Cisco TAC and opening a service request.

SYSTEM (13)

To troubleshoot and correct the cause of the alarm, refer to the "Multiple Readers and Multiple Writers Maximum Q Depth Reached - System (13)" section on page 12-16.

DESCRIPTION	Multiple Readers and Multiple Writers Maximum Queue Depth Reached
SEVERITY	CRITICAL
THRESHOLD	100
THROTTLE	0
DATAWORDS	High Mark for Queue Depth - FOUR_BYTES Low Mark for Queue Depth - FOUR_BYTES
PRIMARY CAUSE	Messages flooding from a malfunctioning network element.
PRIMARY ACTION	Check messages to process.
SECONDARY CAUSE	Resource congestion or slow processing of messages from queue.
SECONDARY ACTION	Check the process and system resources. May need failover.

SYSTEM (14)

To troubleshoot and correct the cause of the alarm, refer to the "Multiple Readers and Multiple Writers Queue Reached Low Queue Depth - System (14)" section on page 12-16.

DESCRIPTION	Multiple Readers and Multiple Writers Queue Reached Low Queue Depth
SEVERITY	MINOR
THRESHOLD	100
THROTTLE	0
DATAWORDS	Lower Queue Depth Limit - FOUR_BYTES Higher Queue Depth Limit - FOUR_BYTES
PRIMARY CAUSE	High rate of messages being received from the network.
PRIMARY ACTION	Check messages to the system.
SECONDARY CAUSE	System or processing thread congestion.
SECONDARY ACTION	Check process and system resources.

SYSTEM (15)

To troubleshoot and correct the cause of the alarm, refer to the "Multiple Readers and Multiple Writers Throttle Queue Depth Reached - System (15)" section on page 16.

DESCRIPTION	Multiple Readers and Multiple Writers Throttle Queue Depth Reached
SEVERITY	MAJOR
THRESHOLD	100
THROTTLE	0
DATAWORDS	Throttle Mark for Queue Depth - FOUR_BYTES Throttle Clear Mark for Queue De - FOUR_BYTES
PRIMARY CAUSE	Inbound network messages arriving at a rate much higher than processing capacity.
PRIMARY ACTION	Determine the cause of increase in inbound network traffic, and try to control the traffic externally.
SECONDARY CAUSE	Resource congestion resulting in a slow down in processing messages from queue.
SECONDARY ACTION	Check the platform CPU utilization, IPC queue depths and overall availability of system resources.

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)	Test Report - System (1)	INFO
SYSTEM(2)	Inter-Process Communication Queue Read Failure - System (2)	MINOR
SYSTEM(3)	Inter-Process Communication Message Allocate Failure - System (3)	MINOR
SYSTEM(4)	Inter-Process Communication Message Send Failure - System (4)	MINOR
SYSTEM(5)	Unexpected Inter-Process Communication Message Received - System (5)	WARNING
SYSTEM(6)	Index List Insert Error - System (6)	MINOR
SYSTEM(7)	Index List Remove Error - System (7)	MINOR
SYSTEM(8)	Thread Creation Failure - System (8)	MAJOR
SYSTEM(9)	Timer Start Failure - System (9)	WARNING
SYSTEM(10)	Index Update Registration Error - System (10)	MINOR
SYSTEM(11)	Index Table Add-Entry Error - System (11)	MINOR
SYSTEM(12)	Software Error - System (12)	MAJOR
SYSTEM(13)	Multiple Readers and Multiple Writers Maximum Q Depth Reached - System (13)	CRITICAL
SYSTEM(14)	Multiple Readers and Multiple Writers Queue Reached Low Queue Depth - System (14)	MINOR
SYSTEM(15)	Multiple Readers and Multiple Writers Throttle Queue Depth Reached - System (15)	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 12-14.

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 12-14.

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 12-15.

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 Documentation and Submitting a Service Request" section on page liii 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 12-15.

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 12-15.

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 12-15.

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 Documentation and Submitting a Service Request" section on page liii 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 12-15.

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 12-16.

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 12-16.

Multiple Readers and Multiple Writers Maximum Q Depth Reached - System (13)

The Multiple Readers and Multiple Writers Maximum Q Depth Reached alarm (critical) indicates that the multiple readers and multiple writers (MRMW) maximum queue depth has been reached. To troubleshoot and correct the cause of the Multiple Readers and Multiple Writers Maximum Q Depth Reached alarm, refer to the "Multiple Readers and Multiple Writers Maximum Q Depth Reached - System (13)" section on page 12-16.

Multiple Readers and Multiple Writers Queue Reached Low Queue Depth - System (14)

The Multiple Readers and Multiple Writers Queue Reached Low Queue Depth alarm (minor) indicates that the MRMW queue has reached the low queue depth threshold. To troubleshoot and correct the cause of the Multiple Readers and Multiple Writers Queue Reached Low Queue Depth alarm, refer to the "Multiple Readers and Multiple Writers Queue Reached Low Queue Depth - System (14)" section on page 12-16.

Multiple Readers and Multiple Writers Throttle Queue Depth Reached - System (15)

The Multiple Readers and Multiple Writers Throttle Queue Depth Reached alarm (major) indicates that the MRMW queue has reached the throttle depth. To troubleshoot and correct the cause of the Multiple Readers and Multiple Writers Throttle Queue Depth Reached alarm, refer to the "Multiple Readers and Multiple Writers Throttle Queue Depth Reached - System (15)" section on page 16.

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)	Inter-Process Communication Queue Read Failure - System (2)	MINOR
SYSTEM(3)	Inter-Process Communication Message Allocate Failure - System (3)	MINOR
SYSTEM(4)	Inter-Process Communication Message Send Failure - System (4)	MINOR
SYSTEM(6)	Index List Insert Error - System (6)	MINOR
SYSTEM(7)	Index List Remove Error - System (7)	MINOR
SYSTEM(8)	Thread Creation Failure - System (8)	MAJOR
SYSTEM(10)	Index Update Registration Error - System (10)	MINOR
SYSTEM(11)	Index Table Add Entry Error - System (11)	MINOR
SYSTEM(12)	Software Error - System (12)	MAJOR
SYSTEM(13)	Multiple Readers and Multiple Writers Maximum Q Depth Reached - System (13)	CRITICAL
SYSTEM(14)	Multiple Readers and Multiple Writers Queue Reached Low Queue Depth - System (14)	MINOR
SYSTEM(15)	Multiple Readers and Multiple Writers Throttle Queue Depth Reached - System (15)	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 Documentation and Submitting a Service Request" section on page liii 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 Documentation and Submitting a Service Request" section on page liii 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 Documentation and Submitting a Service Request" section on page liii 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 Documentation and Submitting a Service Request" section on page liii 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 Documentation and Submitting a Service Request" section on page liii 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 Documentation and Submitting a Service Request" section on page liii 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 Documentation and Submitting a Service Request" section on page liii 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 Documentation and Submitting a Service Request" section on page liii 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 Documentation and Submitting a Service Request" section on page liii for detailed instructions on contacting Cisco TAC and opening a service request.

Multiple Readers and Multiple Writers Maximum Q Depth Reached - System (13)

The Multiple Readers and Multiple Writers Maximum Q Depth Reached alarm (critical) indicates that the MRMW maximum queue depth has been reached. The primary cause of the alarm is message flooding from an erratic network element. To correct the primary cause of the alarm, check the messages to process, The secondary cause of the alarm is resource congestion or slow processing of messages from queue. To correct the secondary cause of the alarm, check the process and system resources. The system may need to be failed over.

Multiple Readers and Multiple Writers Queue Reached Low Queue Depth - System (14)

The Multiple Readers and Multiple Writers Queue Reached Low Queue Depth alarm (minor) indicates that the MRMW queue has reached the low queue depth threshold. The primary cause of the alarm is a high rate of messages from the network. To correct the primary cause of the alarm, check the messages to the system. The secondary cause of the alarm is system or processing thread congestion. To correct the secondary cause of the alarm, check process and system resources.

Multiple Readers and Multiple Writers Throttle Queue Depth Reached - System (15)

The Multiple Readers and Multiple Writers Throttle Queue Depth Reached alarm (major) indicates that the MRMW queue has reached the throttle depth. The primary cause of the alarm is that inbound network messages arriving at a rate much higher than processing capacity. To correct the primary cause of the alarm, determine the cause of increase in inbound network traffic, and try to control the traffic externally. The secondary cause of the alarm is that there is resource congestion resulting in a slow down in processing messages from queue. To correct the secondary cause of the alarm, check the platform CPU utilization, IPC queue depths and overall availability of system resources.

CHAPTER 13

Network Troubleshooting

Revised: July 22, 2009, OL-8000-32

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 13-7
- Oracle Database Tool Restart, 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
                                                          Effect Primary
ASP Name      AS Name       State           Type  Rmt Port Remote IP 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
```

a. 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
```

b. If the status of the ASP is inactive, the ASP is probably on the standby Cisco BTS 10200 Softswitch.

c. 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
```

d. 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:

a. Correct the mismatch.

b. Bounce the SCTP association on the Cisco BTS 10200 Softswitch.

c. 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:

a. Correct it in the /etc/hosts file and on the domain name system (DNS) server, if necessary.

b. Correct it on the ITP if the IP addresses on the ITP are incorrect.

c. Bounce the SCTP association on the Cisco BTS 10200 Softswitch.

d. 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:

a. If the interface is down, shut down the interface manually.

b. If the line protocol is down, the problem exists in cabling or in the MTP2 layer.

c. 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.

Oracle Database Tool Restart

After a network failure, if dbadm tool indicates that database jobs 3, 4, 5,and 6 are broken, the database administrator needs to restart the jobs using the following procedure.

Step 1 Login to oracle.

```
su - oracle
```

Step 2 Restart database job 3.

```
$ java dba.rep.RepAdmin -enable job 3
```

Step 3 Restart database job 4.

```
$ java dba.rep.RepAdmin -enable job 4
```

Step 4 Restart database job 5.

```
$ java dba.rep.RepAdmin -enable job 5
```

Step 5 Restart database job 6.

```
$ java dba.rep.RepAdmin -enable job 6
```

CHAPTER 14

General Troubleshooting

Revised: July 22, 2009, OL-8000-32

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.
- File Configuration – bts.properties - Provides instructions for editing and configuring the bts.properties file.
- Privacy Screening Troubleshooting - Provides instructions for troubleshooting privacy screening.

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 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 cases, as applicable:

- Verify that Alerting Notification is included in the SERVICE table applicable to the specific subscriber.
- Verify that Alerting Notification is included in the SERVICE table applicable to the specific POP (the service ID identified by the office-service-id token in the POP table).
- Verify that Alerting Notification is included in the default office service ID (if the feature is intended to be offered by default 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:

Step 1 Log on to the ITP, and get into configure mode.

Step 2 Type the first configuration line of the resource that you want to control.

Step 3 Type **shut** to take the resource out of service, or type **no-shut** 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

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

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 NTP3/2/1, 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 Chapter 13, "Network Troubleshooting," 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_bcsm_util.c:2614]
[***ERROR*** 10:40:00.299 BCM  01-1 BCM_Main   ]  "Route Selection Failure"
[bcm_obcsm_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	RASSignalAddr	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(pcld=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 IDSN 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.

a. 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).

b. 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 14-34

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 xxxxxxx
!
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-l3 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 tsmax 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 the instructions for extracting the bts.properties file from the util.jar file and for editing and changing configuration information in the extracted bts.properties file. The default content of 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
logBakupSuffix=	.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

Table 14-1 Default Content of the bts.properties File.

Parameter	Variable
invalidChars=	"'; **Note** # spaces or other white space characters may be considered invalid.
LERGDuration=	86400000
throttleEnable=	N

File Extraction and Editing – bts.properties

Prior to extraction, the bts.properties file is part of the util.jar file. To change any of the bts.properties file parameters, it must be extracted from the util.jar file. Use the following instructions to extract the bts.properteries file from the util.jar file and to edit the extracted bts.properties file.

Step 1 Locate the util.jar file and unjar it.

Step 2 Locate to the bts.properties file in the directory that was unjared in Step 1.

Step 3 Edit the bts.properties file to change the desired parameter(s).

Step 4 Rejar the whole directory containing the bts.properties file.

Step 5 Replace the old util.jar file with the new util.jar file created in Step 4.

Step 6 Shutdown and restart the affected processes.

Privacy Screening Troubleshooting

This section lists several privacy screening troubleshooting symptoms and solutions.

Symptom One

With a Cisco 2421, calls are placed, but PRIVACY SCREENING is not displayed on the caller-id display for the subscriber.

Solution One

Telnet to the Cisco 2421 and set dtmf-relay mode to nse. For example, execute the following command in config mode:

```
mgcp dtmf-relay voip codec all mode nse
```

Symptom Two

The caller or the subscriber is on a Cisco ATA MGW and CRCX/MGCX is failing.

Solution Two

Either the PS feature or the PS_MANAGE feature is working but not both.

For the trunk group against the DN that is mapped to the PS App, verify that the softsw-tsap-addr is set to an IP address and not a domain name. For the trunk group against the DN that is mapped to the PS_MANAGE App, verify that the softsw-tsap-addr is set to a domain name and not an IP address.

Symptom Three

Privacy Screening is not able to collect digits or record with a Cisco 2421.

Solution Three

In the Cisco 2421 media gateway, execute the following command:

```
mgcp rtp payload cisco-pcm-switch-over-ulaw 126
```

Symptom Four

Only one Privacy Screening or Privacy Screening PIN Management application works for a subscriber.

Solution Four

Verify the pilot number of the organization in the Privacy Screening application to which the subscriber belongs. This should match the ACCESS_DN in the app-server table to which the subscriber is associated.

CHAPTER 15

Diagnostic Tests

Revised: July 22, 2009, OL-8000-32

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 15-3
- Signaling System 7 Trunk Termination Tests, page 15-5
- Integrated Services Digital Network Trunk Termination Tests, page 15-8
- Channel-Associated Signaling Trunk Termination Tests, page 15-9
- Announcement Trunk Termination Tests, page 15-11
- Troubleshooting Using Snoop, page 15-12
- Query Verification Tool and Translation Verification Tool, page 15-16
- Network Loopback Test for Network-based Call Signaling/Media Gateway Control Protocol Endpoints, page 15-34
- Session Initiation Protocol Subscriber Registration Status Check, page 15-41
- System Health Report, page 15-42
- Fast Audit and Sync Tool, page 15-42
- ISDN Network Loopback Test, page 15-44
- Enhanced Traffic Measurement, page 15-53
- PSTN Trunk Testing, page 15-80

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.
```

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.

Step 4 Force the subscriber termination into INS state:

```
control subscriber-termination id=sub2-ctx2; mode=forced; target-state=ins;
```

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

Response	Description
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 INS state:

```
control isdn-trunk-termination tgn-id=17; mode=forced; target-state=ins;
```

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 annc-trunk-termination tgn-id=13; mode=forced; target-state=maint;
```

Step 2 Display the Test Menu.

```
diag annc-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 annc-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 annc-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 annc-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 annc-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>
 recvpipe  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>
 recvpipe  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>
 recvpipe  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>
 recvpipe  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-itpa
SGP_ID=sgp1
SCTP_ASSOC_PROFILE_ID=sctp-prof1
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-itpa
SGP_ID=sgp2
SCTP_ASSOC_PROFILE_ID=sctp-prof1
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 15-16
- Query Verification Tool, page 15-16
- Translation Verification Tool, page 15-22
- Using Query Verification Tool and Translation Verification Tool Together, page 15-25

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 15-17
- Command Format, page 15-17
- Response Format, page 15-18

- Query Errors, page 15-19
- Query Verification Tool Measurements, page 15-22

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)/1 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/1 queries.
* Called-DN	
* LATA	Local access and transport area. VARCHAR (5)
Originating Line Information (OLI)	Optional parameter used if the message-type is IN/1. 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;

Syntax Description

* 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 lidb; 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 lidb; 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 lidb? 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 subs system, 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 lidb; 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 15-23
- Command Format, page 15-23
- Response Format, page 15-23
- Translation Verification Tool Measurements, page 15-24

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

Syntax Description

* 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;

Syntax Description

* 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=ssp1dest;SPLIT_NPA=NONE;DEL_DIGITS=0;MIN_DIGITS=10;MAX_
DIGITS=10;NOA=NATIONAL;

TABLE: DESTINATION
DEST_ID=ssp1dest;CALL_TYPE=LOCAL;ROUTE_TYPE=ROUTE;ROUTE_GUIDE_ID=ssp1rg;ZERO_PLUS=N;INTRA_
STATE=Y;GAP_ROUTING=N;CLDPTY_CTRL_REL_ALWD=N;TABLE: ROUTE_GUIDE
ID=ssp1rg;POLICY_TYPE=ROUTE;POLICY_ID=ssp1route;

TABLE: ROUTE
ID=ssp1route;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-pro
f;STATUS=INS;DIRECTION=BOTH;SEL_POLICY=ASC;GLARE=EVEN;ALT_ROUTE_ON_CONG=N;SIGNAL_PORTED_NU
MBER=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;C
ALL_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_DIGITS
5=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-pro
f;STATUS=INS;DIRECTION=BOTH;SEL_POLICY=ASC;GLARE=EVEN;ALT_ROUTE_ON_CONG=N;SIGNAL_PORTED_NU
MBER=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;C
ALL_CTRL_ROUTE_ID=bts12-ccroute1;MGCP_PKG_TYPE=T;ANI_SCREENING=N;SEND_RDN_AS_CPN=N;

Reply : Success:

CLI>
```

LNP Examples

The following examples illustrate typical LNP call scenarios:

Example 1

This example illustrates a TVT command on a trunk origination, with CdPN resulting in an LNP query. QVT gets the RN and suggests the second translate command. The second TVT shows the route of the outgoing trunk group to the recipient switch.

```
btsadmin>translate trunk tgn-id=5; called-dn=11501160;

TRANSLATE ON CALL AGENT CA146 IS... ->

TABLEINFO ->
TABLE: TRUNK_GRP

ID=5;CALL_AGENT_ID=CA146;TG_TYPE=SS7;NUM_OF_TRUNKS=24;DPC=5-2-3;TG_PROFI
LE_ID=tgprof_inet116;STATUS=INS;DIRECTION=IN;SEL_POLICY=DSC;GLARE=SLAVE;
ALT_ROUTE_ON_CONG=N;SIGNAL_PORTED_NUMBER=Y;POP_ID=hun1;DIAL_PLAN_ID=dp_t
rk_itu;DESCRIPTION=TG IN from Inet
```

```
116;DEL_DIGITS=0;TRAFFIC_TYPE=LOCAL;ANI_BASED_ROUTING=N;CALL_CTRL_ROUTE_
ID=cc_rte_i116_tg5;MGCP_PKG_TYPE=T;ANI_SCREENING=N;SEND_RDN_AS_CPN=N;STA
TUS_MONITORING=N;SEND_EARLY_BKWD_MSG=N;EARLY_BKWD_MSG_TMR=5;SCRIPT_SUPP=
N;VOICE_LAYER1_USERINFO=AUTO;VOICE_INFO_TRANSFER_CAP=AUTO;ACCESS_TYPE=CO
MBINED;POI=INTER_ENDOFFICE;PERFORM_LNP_QUERY=Y;

TABLE: DIAL_PLAN_PROFILE

     .
     .
     .

TABLE: OFFICE_CODE

DIGIT_STRING=11501;OFFICE_CODE_INDEX=15;DID=N;CALL_AGENT_ID=CA146;DIALAB


LE=Y;NDC=1;EC=150;DN_GROUP=1xxx;EC_DIGIT_STRING=1150;

TABLE: DN2SUBSCRIBER

OFFICE_CODE_INDEX=15;DN=1160;STATUS=PORTED_OUT;RING_TYPE=1;LNP_TRIGGER=N
;NP_RESERVED=N;LAST_CHANGED=2005-08-11
14:30:09.0;VIRTUAL_DN=N;PORTED_IN=N;

 ****** THIS CALL NEEDS AN LNP QUERY ******

****** LNP QUERY is needed (Onward Call Routing query), Suggested QUERY


Command to Run ******

QUERY LNP;tgn-id=5; called-dn=11501160

****** If query result is Routing Number (RN) Not Found,

       the above translation is valid

****** Otherwise, use the TRANSLATE command

       suggested by the query result



Reply : Success:


btsadmin>QUERY LNP; tgn-id=5; called-dn=11501160;

QUERY ON FEATURE SERVER FSAIN205 IS... ->

RESULT ->
Called Number=11501160, Routing Number (RN) =4101
**** Suggested TRANSLATE Command ****

TRANSLATE TRUNK tgn_id=5; original_called_dn=11501160;
called_dn=4101-11501160; noa=PORTED_NUMBER_WITH_RN;

btsadmin>TRANSLATE TRUNK tgn_id=5; original_called_dn=11501160;
called_dn=4101-11501160; noa=PORTED_NUMBER_WITH_RN;

TRANSLATE ON CALL AGENT CA146 IS... ->

TABLEINFO ->
```

```
TABLE: TRUNK_GRP

     .
     .
     .


ID=inet116_rg1;POLICY_TYPE=ROUTE;POLICY_ID=inet116_rte;

TABLE:  ROUTE

ID=inet116_rte;TGN1_ID=6;DEL_DIGITS1=0;DEL_DIGITS2=0;DEL_DIGITS3=0;DEL_D
IGITS4=0;DEL_DIGITS5=0;DEL_DIGITS6=0;DEL_DIGITS7=0;DEL_DIGITS8=0;DEL_DIG
ITS9=0;DEL_DIGITS10=0;TG_SELECTION=SEQ;NEXT_ACTION=NONE;

TABLE: TRUNK_GRP

ID=6;CALL_AGENT_ID=CA146;TG_TYPE=SS7;NUM_OF_TRUNKS=24;DPC=5-2-4;TG_PROFI
LE_ID=tgprof_inet116;STATUS=INS;DIRECTION=OUT;SEL_POLICY=DSC;GLARE=SLAVE
;ALT_ROUTE_ON_CONG=N;SIGNAL_PORTED_NUMBER=Y;POP_ID=hun1;DIAL_PLAN_ID=dp_
trk_itu;DESCRIPTION=TG OUT to Inet
116;DEL_DIGITS=0;TRAFFIC_TYPE=LOCAL;ANI_BASED_ROUTING=N;CALL_CTRL_ROUTE_
ID=cc_rte_i116_tg6;MGCP_PKG_TYPE=T;ANI_SCREENING=N;SEND_RDN_AS_CPN=N;STA
TUS_MONITORING=N;SEND_EARLY_BKWD_MSG=N;EARLY_BKWD_MSG_TMR=5;SCRIPT_SUPP=
N;VOICE_LAYER1_USERINFO=AUTO;VOICE_INFO_TRANSFER_CAP=AUTO;ACCESS_TYPE=CO
MBINED;POI=INTER_ENDOFFICE;PERFORM_LNP_QUERY=N;



Reply : Success:
```

Example 2

In this example, a subscriber dials an DN ported-out of this switch. QVT gets the RN, and a second TVT shows the route of the outgoing trunk group to the recipient switch.

Because the called DN is ported-out, the call cannot be routed on this switch without an LNP query. If QVT does not find an RN, perhaps because the DN2RN table is incorrect temporarily during the porting transition, the call will be released due to cause unallocated number.

```
btsadmin>translate line calling-dn=11501511; called-dn=11501160;

TRANSLATE ON CALL AGENT CA146 IS... ->

TABLEINFO ->

TABLE: SUBSCRIBER

ID=sipata1;CATEGORY=INDIVIDUAL;NAME=h15 sipata1
Moe;STATUS=ACTIVE;BILLING_DN=11501511;DN1=11501511;PRIVACY=NONE;RING_TYPE_DN1=1;PIC1=NONE;
PIC2=NONE;PIC3=NONE;GRP=N;USAGE_SENS=Y;SUB_PROFILE_ID=hungary_prof;TERM_TYPE=SIP;IMMEDIATE
_RELEASE=N;TERMINATING_IMMEDIATE_REL=N;AOR_ID=11501511@192.168.54.124;SEND_BDN_AS_CPN=N;SE
ND_BDN_FOR_EMG=N;PORTED_IN=N;BILLING_TYPE=NONE;VMWI=Y;SDT_MWI=Y;


     .
     .
     .

TABLE: DN2SUBSCRIBER
```

```
OFFICE_CODE_INDEX=15;DN=1160;STATUS=PORTED_OUT;RING_TYPE=1;LNP_TRIGGER=N;NP_RESERVED=N;LAS
T_CHANGED=2005-08-11 14:30:09.0;VIRTUAL_DN=N;PORTED_IN=N;

 ****** THIS CALL NEEDS AN LNP QUERY ******

****** LNP QUERY is needed (Onward Call Routing query), Suggested QUERY Command to Run
******

QUERY LNP;calling-dn=11501511;called-dn=11501160

****** If query result is Routing Number (RN) Not Found,

       the above translation is valid

****** Otherwise, use the TRANSLATE command

       suggested by the query result



Reply : Success:

btsadmin>
btsadmin>
btsadmin>QUERY LNP;calling-dn=11501511;called-dn=11501160

QUERY ON FEATURE SERVER FSAIN205 IS... ->

RESULT ->
Called Number=11501160, Routing Number (RN) =4101
**** Suggested TRANSLATE Command ****

TRANSLATE LINE calling_dn=11501511; original_called_dn=11501160; called_dn=4101-11501160;
NOA=PORTED-NUMBER-WITH-RN;

QUERYSTATUS -> Query Success

Reply : Success:

btsadmin>
btsadmin>
btsadmin>TRANSLATE LINE calling_dn=11501511; original_called_dn=11501160;
called_dn=4101-11501160; NOA=PORTED-NUMBER-WITH-RN;

TRANSLATE ON CALL AGENT CA146 IS... ->

TABLEINFO ->

TABLE: SUBSCRIBER

ID=sipata1;CATEGORY=INDIVIDUAL;NAME=h15 sipata1
Moe;STATUS=ACTIVE;BILLING_DN=11501511;DN1=11501511;PRIVACY=NONE;RING_TYPE_DN1=1;PIC1=NONE;
PIC2=NONE;PIC3=NONE;GRP=N;USAGE_SENS=Y;SUB_PROFILE_ID=hungary_prof;TERM_TYPE=SIP;IMMEDIATE
_RELEASE=N;TERMINATING_IMMEDIATE_REL=N;AOR_ID=11501511@192.168.54.124;SEND_BDN_AS_CPN=N;SE
ND_BDN_FOR_EMG=N;PORTED_IN=N;BILLING_TYPE=NONE;VMWI=Y;SDT_MWI=Y;


     .
     .
     .


TABLE: TRUNK_GRP
```

```
ID=6;CALL_AGENT_ID=CA146;TG_TYPE=SS7;NUM_OF_TRUNKS=24;DPC=5-2-4;TG_PROFILE_ID=tgprof_inet1
16;STATUS=INS;DIRECTION=OUT;SEL_POLICY=DSC;GLARE=SLAVE;ALT_ROUTE_ON_CONG=N;SIGNAL_PORTED_N
UMBER=Y;POP_ID=hun1;DIAL_PLAN_ID=dp_trk_itu;DESCRIPTION=TG OUT to Inet
116;DEL_DIGITS=0;TRAFFIC_TYPE=LOCAL;ANI_BASED_ROUTING=N;CALL_CTRL_ROUTE_ID=cc_rte_i116_tg6
;MGCP_PKG_TYPE=T;ANI_SCREENING=N;SEND_RDN_AS_CPN=N;STATUS_MONITORING=N;SEND_EARLY_BKWD_MSG
=N;EARLY_BKWD_MSG_TMR=5;SCRIPT_SUPP=N;VOICE_LAYER1_USERINFO=AUTO;VOICE_INFO_TRANSFER_CAP=A
UTO;ACCESS_TYPE=COMBINED;POI=INTER_ENDOFFICE;PERFORM_LNP_QUERY=N;



Reply : Success:
btsadmin>
```

Example 3

In this example, the first TVT shows a translation but indicates that an LNP query is needed. The QVT does not find an RN, so the first TVT has the correct translation and routing information.

```
btsadmin>translate line calling-dn=11501511; called-dn=11501512;

TRANSLATE ON CALL AGENT CA146 IS... ->

TABLEINFO ->

TABLE: SUBSCRIBER

ID=sipata1;CATEGORY=INDIVIDUAL;NAME=h15 sipata1
Moe;STATUS=ACTIVE;BILLING_DN=11501511;DN1=11501511;PRIVACY=NONE;RING_TYPE_DN1=1;PIC1=NONE;
PIC2=NONE;PIC3=NONE;GRP=N;USAGE_SENS=Y;SUB_PROFILE_ID=hungary_prof;TERM_TYPE=SIP;IMMEDIATE
_RELEASE=N;TERMINATING_IMMEDIATE_REL=N;AOR_ID=11501511@192.168.54.124;SEND_BDN_AS_CPN=N;SE
ND_BDN_FOR_EMG=N;PORTED_IN=N;BILLING_TYPE=NONE;VMWI=Y;SDT_MWI=Y;

TABLE: SUBSCRIBER_PROFILE

ID=hungary_prof;DIAL_PLAN_ID=dp_sub_itu;LOCAL_PFX1_OPT=NR;TOLL_PFX1_OPT=RQ;POP_ID=hun1;OLI
=0;EA_USE_PIC1=Y;INTERLATA_PFX1_OPT=RQ;


     .
     .
     .

TABLE: SUBSCRIBER

ID=sipata2;CATEGORY=INDIVIDUAL;NAME=h15 sipata2
Larry;STATUS=ACTIVE;BILLING_DN=11501512;DN1=11501512;PRIVACY=NONE;RING_TYPE_DN1=1;PIC1=NON
E;PIC2=NONE;PIC3=NONE;GRP=N;USAGE_SENS=Y;SUB_PROFILE_ID=hungary_prof;TERM_TYPE=SIP;IMMEDIA
TE_RELEASE=N;TERMINATING_IMMEDIATE_REL=N;AOR_ID=11501512@192.168.54.124;SEND_BDN_AS_CPN=N;
SEND_BDN_FOR_EMG=N;PORTED_IN=N;BILLING_TYPE=NONE;VMWI=Y;SDT_MWI=Y;

****** LNP QUERY is needed (LNP-TRIGGER for ODBR), Suggested QUERY Command to Run ******

QUERY LNP;calling-dn=11501511;called-dn=11501512

****** If query result is Routing Number (RN) Not Found,

       the above translation is valid

****** Otherwise, use the TRANSLATE command

       suggested by the query result
```

```
Reply : Success:

btsadmin>
btsadmin>QUERY LNP;calling-dn=11501511;called-dn=11501512

QUERY ON FEATURE SERVER FSAIN205 IS... ->

RESULT ->
Called Number=11501512, Routing Number (RN) Not Found

QUERYSTATUS -> Query Success

Reply : Success:
```

Example 4

This example is for a QOR originating switch. A subscriber dials a DN that is ported-out of another (donor) switch. The call is translated and routed to the donor switch, as shown in the first translate (TVT) command below. The donor switch sends a REL with LNP QOR: Ported Number cause to the originating switch.

The originating switch receives the REL with LNP QOR: Ported Number cause, and then the originating switch does an LNP query. The QVT query finds an RN, and the RN and NOA are used as input to the TVT to show the routing after the QOR query, as shown in the second translated command below.

```
btsadmin>translate line calling-dn=11501511; called-dn=11161168

TRANSLATE ON CALL AGENT CA146 IS... ->

TABLEINFO ->

TABLE: SUBSCRIBER

ID=sipata1;CATEGORY=INDIVIDUAL;NAME=h15 sipata1
Moe;STATUS=ACTIVE;BILLING_DN=11501511;DN1=11501511;PRIVACY=NONE;RING_TYPE_DN1=1;PIC1=NONE;
PIC2=NONE;PIC3=NONE;GRP=N;USAGE_SENS=Y;SUB_PROFILE_ID=hungary_prof;TERM_TYPE=SIP;IMMEDIATE
_RELEASE=N;TERMINATING_IMMEDIATE_REL=N;AOR_ID=11501511@192.168.54.124;SEND_BDN_AS_CPN=N;SE
ND_BDN_FOR_EMG=N;PORTED_IN=N;BILLING_TYPE=NONE;VMWI=Y;SDT_MWI=Y;

TABLE: SUBSCRIBER_PROFILE

ID=hungary_prof;DIAL_PLAN_ID=dp_sub_itu;LOCAL_PFX1_OPT=NR;TOLL_PFX1_OPT=RQ;POP_ID=hun1;OLI
=0;EA_USE_PIC1=Y;INTERLATA_PFX1_OPT=RQ;


     .
     .
     .

TABLE: TRUNK_GRP

ID=6;CALL_AGENT_ID=CA146;TG_TYPE=SS7;NUM_OF_TRUNKS=24;DPC=5-2-4;TG_PROFILE_ID=tgprof_inet1
16;STATUS=INS;DIRECTION=OUT;SEL_POLICY=DSC;GLARE=SLAVE;ALT_ROUTE_ON_CONG=N;SIGNAL_PORTED_N
UMBER=Y;POP_ID=hun1;DIAL_PLAN_ID=dp_trk_itu;DESCRIPTION=TG OUT to Inet
116;DEL_DIGITS=0;TRAFFIC_TYPE=LOCAL;ANI_BASED_ROUTING=N;CALL_CTRL_ROUTE_ID=cc_rte_i116_tg6
;MGCP_PKG_TYPE=T;ANI_SCREENING=N;SEND_RDN_AS_CPN=N;STATUS_MONITORING=N;SEND_EARLY_BKWD_MSG
=N;EARLY_BKWD_MSG_TMR=5;SCRIPT_SUPP=N;VOICE_LAYER1_USERINFO=AUTO;VOICE_INFO_TRANSFER_CAP=A
UTO;ACCESS_TYPE=COMBINED;POI=INTER_ENDOFFICE;PERFORM_LNP_QUERY=N;
```

```
Reply : Success:

btsadmin>
btsadmin>
btsadmin>
btsadmin>
btsadmin>query LNP; calling-dn=11501511; called-dn=11161168;

QUERY ON FEATURE SERVER FSAIN205 IS... ->

RESULT ->
Called Number=11161168, Routing Number (RN) =4001
**** Suggested TRANSLATE Command ****

TRANSLATE LINE calling_dn=11501511; original_called_dn=11161168; called_dn=4001-11161168;
NOA=PORTED-NUMBER-WITH-RN;

QUERYSTATUS -> Query Success

Reply : Success:

btsadmin>
btsadmin>
btsadmin>
btsadmin>
btsadmin>TRANSLATE LINE calling_dn=11501511; original_called_dn=11161168;
called_dn=4001-11161168; NOA=PORTED-NUMBER-WITH-RN;

TRANSLATE ON CALL AGENT CA146 IS... ->

TABLEINFO ->

TABLE: SUBSCRIBER

ID=sipata1;CATEGORY=INDIVIDUAL;NAME=h15 sipata1
Moe;STATUS=ACTIVE;BILLING_DN=11501511;DN1=11501511;PRIVACY=NONE;RING_TYPE_DN1=1;PIC1=NONE;
PIC2=NONE;PIC3=NONE;GRP=N;USAGE_SENS=Y;SUB_PROFILE_ID=hungary_prof;TERM_TYPE=SIP;IMMEDIATE
_RELEASE=N;TERMINATING_IMMEDIATE_REL=N;AOR_ID=11501511@192.168.54.124;SEND_BDN_AS_CPN=N;SE
ND_BDN_FOR_EMG=N;PORTED_IN=N;BILLING_TYPE=NONE;VMWI=Y;SDT_MWI=Y;

TABLE: SUBSCRIBER_PROFILE

ID=hungary_prof;DIAL_PLAN_ID=dp_sub_itu;LOCAL_PFX1_OPT=NR;TOLL_PFX1_OPT=RQ;POP_ID=hun1;OLI
=0;EA_USE_PIC1=Y;INTERLATA_PFX1_OPT=RQ;


     .
     .
     .

TABLE: TRUNK_GRP

ID=6;CALL_AGENT_ID=CA146;TG_TYPE=SS7;NUM_OF_TRUNKS=24;DPC=5-2-4;TG_PROFILE_ID=tgprof_inet1
16;STATUS=INS;DIRECTION=OUT;SEL_POLICY=DSC;GLARE=SLAVE;ALT_ROUTE_ON_CONG=N;SIGNAL_PORTED_N
UMBER=Y;POP_ID=hun1;DIAL_PLAN_ID=dp_trk_itu;DESCRIPTION=TG OUT to Inet
116;DEL_DIGITS=0;TRAFFIC_TYPE=LOCAL;ANI_BASED_ROUTING=N;CALL_CTRL_ROUTE_ID=cc_rte_i116_tg6
;MGCP_PKG_TYPE=T;ANI_SCREENING=N;SEND_RDN_AS_CPN=N;STATUS_MONITORING=N;SEND_EARLY_BKWD_MSG
=N;EARLY_BKWD_MSG_TMR=5;SCRIPT_SUPP=N;VOICE_LAYER1_USERINFO=AUTO;VOICE_INFO_TRANSFER_CAP=A
UTO;ACCESS_TYPE=COMBINED;POI=INTER_ENDOFFICE;PERFORM_LNP_QUERY=N;

Reply : Success:
```

Example 5

This example illustrates an incoming trunk call with an RN prefix and ported number NOA.

Note In this example, the BTS10200 reminds you that the NOA and ORIGINAL-CALLED-DN tokens must both be specified.

```
btsadmin>translate trunk tgn-id=5; called-dn=400111501512; NOA=PORTED-NUMBER-WITH-RN;

Reply : Failure: NOA and ORIGINAL-CALLED-DN should be specified together

btsadmin>
btsadmin>
btsadmin>translate trunk tgn-id=5; called-dn=400111501512; NOA=PORTED-NUMBER-WITH-RN;
original-called-dn=11501512;

TRANSLATE ON CALL AGENT CA146 IS... ->

TABLEINFO ->
TABLE: TRUNK_GRP

ID=5;CALL_AGENT_ID=CA146;TG_TYPE=SS7;NUM_OF_TRUNKS=24;DPC=5-2-3;TG_PROFILE_ID=tgprof_inet1
16;STATUS=INS;DIRECTION=IN;SEL_POLICY=DSC;GLARE=SLAVE;ALT_ROUTE_ON_CONG=N;SIGNAL_PORTED_NU
MBER=Y;POP_ID=hun1;DIAL_PLAN_ID=dp_trk_itu;DESCRIPTION=TG IN from Inet
116;DEL_DIGITS=0;TRAFFIC_TYPE=LOCAL;ANI_BASED_ROUTING=N;CALL_CTRL_ROUTE_ID=cc_rte_i116_tg5
;MGCP_PKG_TYPE=T;ANI_SCREENING=N;SEND_RDN_AS_CPN=N;STATUS_MONITORING=N;SEND_EARLY_BKWD_MSG
=N;EARLY_BKWD_MSG_TMR=5;SCRIPT_SUPP=N;VOICE_LAYER1_USERINFO=AUTO;VOICE_INFO_TRANSFER_CAP=A
UTO;ACCESS_TYPE=COMBINED;POI=INTER_ENDOFFICE;PERFORM_LNP_QUERY=Y;

TABLE: DIAL_PLAN_PROFILE

ID=dp_trk_itu;DESCRIPTION=Trunk Origination Local dial-plan
(ITU);NANP_DIAL_PLAN=N;ANI_DIGMAN_ID=dm_dpp_ani_itu;DNIS_DIGMAN_ID=dm_dpp_trk_itu;OVERDECA
DIC_DIGITS_SUPP=N;NOA_BASED_ROUTING=Y;NOA_ROUTE_PROFILE_ID=noa_rt;

TABLE: DIGMAN

ID=dm_dpp_ani_itu;RULE=1;MATCH_NOA=ANY;REPLACE_NOA=NATIONAL;

TABLE: DIGMAN

ID=dm_dpp_trk_itu;RULE=1;MATCH_STRING=^4001;REPLACE_STRING=NONE;MATCH_NOA=PORTED_NUMBER_WI
TH_RN;REPLACE_NOA=UNKNOWN;

TABLE: NOA_ROUTE_PROFILE

ID=noa_rt;DESCRIPTION=NOA Route profile (ITU) to RN dial-plan;

CONTINUE WITH EXISTING DIAL-PLAN

TABLE: DIAL_PLAN

ID=dp_trk_itu;DIGIT_STRING=1150;DEST_ID=dest_sub_itu;SPLIT_NPA=NONE;DEL_DIGITS=0;MIN_DIGIT
S=8;MAX_DIGITS=8;NOA=UNKNOWN;

TABLE: DESTINATION
```

```
DEST_ID=dest_sub_itu;CALL_TYPE=LOCAL;ROUTE_TYPE=SUB;ZERO_PLUS=N;INTRA_STATE=Y;DESCRIPTION=
ITU Sub dest: Allow LNP
query;GAP_ROUTING=N;ANI_DIGMAN_ID=dm_dest_sub_ani;DNIS_DIGMAN_ID=dm_dest_rn;CLDPTY_CTRL_RE
L_ALWD=N;CALL_SUBTYPE=NONE;ACQ_LNP_QUERY=PERFORM_LNP_QUERY;

TABLE: OFFICE_CODE

DIGIT_STRING=11501;OFFICE_CODE_INDEX=15;DID=N;CALL_AGENT_ID=CA146;DIALABLE=Y;NDC=1;EC=150;
DN_GROUP=1xxx;EC_DIGIT_STRING=1150;

TABLE: DN2SUBSCRIBER

OFFICE_CODE_INDEX=15;DN=1512;STATUS=ASSIGNED;RING_TYPE=1;LNP_TRIGGER=Y;NP_RESERVED=N;SUB_I
D=sipata2;LAST_CHANGED=2005-09-08 11:08:47.0;VIRTUAL_DN=N;PORTED_IN=N;

TABLE: SUBSCRIBER

ID=sipata2;CATEGORY=INDIVIDUAL;NAME=h15 sipata2
Larry;STATUS=ACTIVE;BILLING_DN=11501512;DN1=11501512;PRIVACY=NONE;RING_TYPE_DN1=1;PIC1=NON
E;PIC2=NONE;PIC3=NONE;GRP=N;USAGE_SENS=Y;SUB_PROFILE_ID=hungary_prof;TERM_TYPE=SIP;IMMEDIA
TE_RELEASE=N;TERMINATING_IMMEDIATE_REL=N;AOR_ID=11501512@192.168.54.124;SEND_BDN_AS_CPN=N;
SEND_BDN_FOR_EMG=N;PORTED_IN=N;BILLING_TYPE=NONE;VMWI=Y;SDT_MWI=Y;


Reply : Success:

btsadmin>
```

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 BTS 10200.

The basic network loopback test feature which was implemented in Release 4.4 is service affecting. In other words, while a network loopback call is in progress, the endpoint is considered busy.

In this release, the BTS 10200 network loopback and network continuity tests also has a service not affected mode. In this mode, the BTS 10200 will attempt to create coexisting test connection on the test device, however if the endpoint does not have enough resources the BTS 10200 will provide preference to regular calls over any test calls.

In the service affected mode the BTS 10200 will not try to perform other calls, even if the test MTA/TGW has capability to perform multiple connections (PARALLEL-TEST-CONN-SUPP=Y).

The BTS 10200 allows the system level configuration to specify whether the network loopback and network continuity test calls will be service affecting or not service affecting.

Restrictions

Although you can test this feature by using the regular MTA as the testing device by configuring the endpoints as subscriber terminations in BTS 10200, 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 BTS 10200 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

In order for parallel test connections to work, the following settings need to be configured in the ca-config:

```
add ca-config type=NLB-TEST-SERVICE-AFFECTING; datatype=BOOLEAN; value=N;
add ca-config type=NCT-TEST-SERVICE-AFFECTING; datatype=BOOLEAN; value=N;
```

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 *BTS 10200 Command Line Interface Reference Guide*.

Global Configuration Example

Use the following procedure as a global configuration example.

Step 1 Add ca-config NLB-TEST-SERVICE-AFFECTING.

```
add ca-config type=NLB-TEST-SERVICE-AFFECTING; value=N
```

Step 2 Add ca-config NCT-TEST-SERVICE-AFFECTING.

```
add ca-config type=NCT-TEST-SERVICE-AFFECTING; value=N;
```

Step 3 Add ca-config TEST-TRUNK-GRP-DIGITS.

```
add ca-config type=TEST-TRUNK-GRP-DIGITS; value=4;
```

Step 4 Add ca-config TEST-TRUNK-MEMBER-DIGITS.

```
add ca-config type=TEST-TRUNK-MEMBER-DIGITS; value=4;
```

Dedicated NLB Testing Device Configuration Example

Note The following is an example of provisioning a dedicated testing trunk-grp for testing network loop-back on a subscriber line. Change TEST-LINE-TYPE to different values (other than NTE) to change test origination type.

Use the following procedure as a dedicated NLB testing device configuration example.

Step 1 Add MGW profile.

```
add mgw-profile id=BRIX; vendor=Tollgrade; mgcp-version=mgcp_1_0; MGCP-VARIANT=NCS-1-0;
```

Step 2 Add cas-tg-profile.

```
add cas-tg-profile id=BRIX_TG; sig-type=LINE; TEST-LINE=Y; TEST-LINE-TYPE=NLB-LINE-TEST
```

Step 3 Add MGW.

```
add mgw id=brix1; tsap-addr=<mgw DNS / IP address>; mgw-profile-id=BRIX; type=TGW;
call-agent id=CA146;
```

Step 4 Add trunk-grp.

```
add trunk-grp id=100; call-agent-id=CA146; tg-type=CAS; cas-tg-profile=BRIX_TG;
mgcp-pkg-type=LINE
```

Step 5 Add termination.

```
add termination prefix=aaln/; port-start=1; port-end=2; type=TRUNK; mgw-id=c925.172;
```

Step 6 Add trunk.

```
add trunk termination-prefix=aaln/; termination-port-start=1; termination-port-end=2;
cic-start=1; cic-end=2; tgn-id=100
```

Shared Testing Device Configuration Example

Use the following procedure as a shared testing device configuration example.

Step 1 Add MGW profile.

```
add mgw-profile id=BRIX; vendor=Tollgrade; mgcp-version=mgcp_1_0; MGCP-VARIANT=NCS-1-0;
```

Step 2 Add cas-tg-profile.

```
add cas-tg-profile id=BRIX_TG; sig-type=LINE; TEST-LINE=Y; TEST-LINE-TYPE=NTE
```

Step 3 Add MGW.

```
add mgw id=brix1; tsap-addr=<mgw DNS / IP address>; mgw-profile-id=BRIX; type=TGW;
call-agent id=CA146;
```

Step 4 Add trunk-grp.

```
add trunk-grp id=100; call-agent-id=CA146; tg-type=CAS; cas-tg-profile=BRIX_TG;
mgcp-pkg-type=LINE
```

Step 5 Add termination.

```
add termination prefix=aaln/; port-start=1; port-end=2; type=TRUNK; mgw-id=c925.172;
```

Step 6 Add trunk.

```
add trunk termination-prefix=aaln/; termination-port-start=1; termination-port-end=2;
cic-start=1; cic-end=2; tgn-id=100
```

Step 7 Add dial-plan-profile.

```
add dial-plan-profile id=dp1; description=NA_Default;
```

Step 8 Add dial-plan.

```
add dial-plan id=dp1; digit-string=919-392; dest-id=sub; noa=national;
```

Step 9 Add digit-map.

```
add digit-map; id=test;
digit-pattern=[2-9]xx[2-9]xxxxxx|011xxxxxx.T|01xxxxxx.T|101xxxx|#|*xx|11xx|xxxxxxxxxxxxxxx
xxxx; description=default_pattern
```

Step 10 Add subscriber-profile.

```
add subscriber-profile id=subpf1; digit-map-id=test; dial-plan-id=DP1; POP-ID=1;
```

Step 11 Add subscriber.

```
add subscriber id=sub11; sub-profile-id= subpf1; category=individual; term-id=aaln/0;
mgw-id=c925.172; dn1=919-392-1235; name=RTP5;
```

Tested Line Device Configuration Example

Use the following procedure as a tested line device configuration example.

Step 1 Add MGW profile.

```
add mgw-profile id=UBR925; vendor=Cisco; mgcp-version=mgcp_1_0; MGCP-VARIANT=NCS_1_0;
```

Step 2 Add MGW.

```
add mgw id=c925.172; tsap-addr=<mgw DNS / IP address>; mgw-profile-id=UBR925; call-agent
id=CA103;
```

Step 3 Add termination.

```
add termination prefix=aaln/; port-start=0; port-end=1; type=line; mgw-id=c925.172;
mgcp-pkg-type=line-ncs;
```

Step 4 Add destination.

```
add destination dest-id=local-call; route-type=sub; call-type=local;
```

Step 5 Add dial-plan-profile.

```
add dial-plan-profile id=dp1; description=NA_Default;
```

Step 6 Add dial-plan.

```
add dial-plan id=dp1; digit-string=919-392; dest-id=sub; noa=national;
```

Step 7 Add subscriber-profile.

```
add subscriber-profile id=subpf1; dial-plan-id=dp1; pop-id=1;
```

Step 8 Add subscriber.

```
add subscriber id=sub11; sub-profile-id= subpf1; category=individual; term-id=aaln/0;
mgw-id=c925.172; dn1=919-392-1235; name=RTP5;
```

Routing for Shared trunk-grp IP Testing Flow Chart Configuration Example

Use the following procedure as a routing for shared trunk-grp IP testing flow chart configuration example.

Step 1 Add destination.

```
add destination dest-id=DEST_NLB_SUB; call-type=TEST-CALL; call-subtype=NLB-LINE-TEST;
route-type=SUB;

add destination dest-id=DEST_NCT_SUB; call-type=TEST-CALL; call-subtype=NCT-LINE-TEST;
route-type=SUB;

add destination dest-id=DEST_NLB_TRUNK; call-type=TEST-CALL; call-subtype=NLB-TRUNK-TEST;
route-type=ROUTE; route-guide-id=abc

add destination dest-id=DEST_NCT_TRUNK; call-type=TEST-CALL; call-subtype=NCT-TRUNK-TEST;
route-type=ROUTE; route-guide-id=abc
```

Step 2 Add dial-plan-profile.

```
add dial-plan-profile id=test; nanp-dial-plan=N
```

Step 3 Add dial-plan.

```
add dial-plan id=test; digit-string=151; dest-id=DEST_NLB_SUB; min-digits=13;
max-digits=13
```

```
add dial-plan id=test; digit-string=152; dest-id=DEST_NCB_SUB; min-digits=13;
max-digits=13

add dial-plan id=test; digit-string=153; dest-id=DEST_NLB_TRUNK; min-digits=13;
max-digits=13

add dial-plan id=test; digit-string=154; dest-id=DEST_NCT_TRUNK; min-digits=13;
max-digits=13
```

Testing Device Status and Control Flowchart Configuration Example

Use the following procedure as a testing device status and control flowchart configuration example.

Step 1 Control MGW.

```
control mgw id=c925.172; target-state=INS; mode=FORCED;
```

Step 2 Status MGW.

```
status mgw id=c925.172;
```

Step 3 Control trunk-grp.

```
control trunk-grp id=100; call-agent-id=CA146; target-state=INS; mode=forced;
```

Step 4 Equip trunk-termination.

```
equip trunk-termination tgn-id=100; cic=all;
```

Step 5 Control trunk-termination.

```
control trunk-termination tgn-id=100; cic=all; target-state=INS; mode=FORCED;
```

Step 6 Status trunk-termination.

```
status trunk-termination id=100; cic=all;
```

Step 7 Reset trunk-termination.

```
reset trunk-termination id=100; cic=all;
```

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:

Step 1 Add a trunk group for the testing device as CAS trunk group (TRUNK-GRP::TG-TYPE=CAS).

Step 2 Associate the trunk group to CAS-TG-PROFILE specific to network loopback test origination type (CAS-TG-PROFILE::TEST-LINE=Y;
CAS-TG-PROFILE::TEST-LINE-TYPE=NLB-LINE/NCT-LINE/NLB-TRUNK/NCT-TRUNK.

Step 3 Add all test lines in the testing device as trunk termination.

Shared Test Trunk Group

In addition to dedicated test trunk groups, the BTS 10200 allows a shared test trunk group, where the category of the test to be run is specified by the test-prefix. BTS 10200 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 a 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=…>
```

Fast Audit and Sync Tool

The bts_audit and bts_sync process tools consists of running two commands, bts_audit and bts_sync. The bts_audit and bts_sync tools are designed to improve speed and integrity. The tools can audit and synchronize all mismatches between network elements.

These tools are not a part of the CLI, but are unix programs that are run by the root user. They bypass the platform messaging paths and access the EMS, CA, FSPTC, and FSAIN databases directly using database tools. The data is manipulated and updates are applied directly to synchronize the databases.

The bts_audit tool is able to:

- Find tables with mismatches
- Find rows missing in application database

- Find rows missing in EMS database
- Find rows with data mismatches between two databases
- Generate a report that lists these mismatches
- Generate the SQL to be used to correct the mismatches

The bts_sync tool is used to send the generated SQL statements to the appropriate destination to bring the databases into synchronization.

The Cisco BTS 10200 Softswitch Fast Audit and Sync Tools feature consists of two expect shell scripts that use other unix scripts and utilities to perform full-database and table audits of the databases on the various network elements of the system, and synchronize the mismatches found. The bts_audit tool determines the tables when performing full database audit by analyzing the catalog of the CA, FSPTC and FSAIN databases. The scripts will create copies of the data from the tables in a standardized format. The data files are used to generate a checksum for each table. The check sums are compared, and if they are not equal, the network element data file will be transferred to the EMS. On the EMS, the data is compared row by row, and mismatches are printed to a file that may be used by the bts_sync tool to restore synchronization of the table on the network element

Restrictions and Limitations

The Cisco BTS 10200 Softswitch Fast Audit and Sync Tools feature described in this document has the following restrictions and limitations:

- The bts_audit/bts_sync tools are unable to audit and synchronize certain scenarios, such as when a termination record points to an invalid mgw.
- The bts_sync tool should only be run to synchronize the data mismatches between the active platforms.
- If audit is given a list of tables, and a table references a missing row in another table, the mismatch will not be resolved by the sync.

Using the bts_audit Tool

To use the bts_audit tool, log in at the unix root prompt and execute the **bts_audit** command.

Using the bts_sync Tool

To properly use the bts_sync tool, the **bts_audit** command must be executed first. Log in at the unix root prompt and execute the **bts_audit** command. Once the **bts_audit** command is execution is complete, execute the **bts_sync** command to synchronize the system databases.

Command Parameters

This section describes the parameters for the **bts_audit** and **bts_sync** commands. The following is an example of the **bts_audit** command parameters:

Example:

```
bts_audit -ems <ems> -ca <ca> [-platforms <platforms>] [-tables <tables>]
```

Where:

ems is the hostname of the active EMS machine.

ca is the hostname of the active CA machine.

platforms is a list of the platforms to be audited without spaces and separated by commas

tables is a list of tables to be audited without spaces and separated by commas.

Example:

```
bts_audit -ems priems01 -ca prica01 -platforms CA146,FSAIN205 -tables
SUBSCRIBER,MGW_PROFILE
```

The **bts_sync** command takes a list of filenames to be used for correcting errors found by the audit.

Example:

```
bts_sync /opt/ems/report/Audit_CA146_root.sql
```

or

```
bts_sync /opt/ems/report/Audit_*_root.sql
```

Command Responses

The execution of the **bts_audit** command will output a list of database mis-matches found.

Database Out of Synchronization

To troubleshoot database out of synchronization alarms, take the following steps:

Step 1 Log in the system at the unix root prompt.

Step 2 Execute the **bts_audit** command.

Step 3 Once the audit is completed, execute the **bts_sync** command.

ISDN Network Loopback Test

This section describes the Network Loopback (NLB) Test for ISDN PRI trunks (ISDN NLB) feature. Network Loopback Test for ISDN-PRI trunks (ISDN NLB) feature allows operators to conduct network loopback testing originating from shared ISDN PRI trunks. The shared test trunk group accepts both normal and test calls. Test calls are identified by provisioning the call-type and call-subtype tokens in the Destination table.

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 The network loopback test cannot be performed if the status of the subscriber to be tested is **unequipped** (**UEQP**) or **operational-out-of-service** (**OOS**).

Configuring

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 must be configured as one of:
  - nlb-line-test
  - nct-line-test
  - nlb-trunk-test
  - nct-trunk-test

Originating Trunk Group

The ISDN NLB feature uses a shared test trunk group, where the type of test 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 is an ISDN PRI trunk. Incoming calls from the network on an ISDN PRI trunk are analyzed according to a preconfigured 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—but the first digit cannot be "1", the Cisco BTS 10200 Softswitch performs the longest match) of the test prefix and its length.
- <Test-data> is a string that depends on the test-prefix content. The following steps configure the originating trunk group:

Step 1 Add a trunk-group for the testing device as an ISDN PRI trunk-group if it does not already exist.

```
trunk-grp::tg-type=isdn;
```

Step 2 Configure the test dial plan destination with the exact type of test call.

Step 3 Configure a main subscriber ID for the testing trunk group if necessary.

Call Agent Configuration Table

The system defaults for the Call Agent Configuration (ca-config) table may require changing, based on the needs of the test.

Step 1 Change service affecting for either NCT or NLB testing. The default is Y.

```
change ca-config::nct-test-service-affecting=n;
change ca-config::nlb-test-service-affecting=n;
```

- Y—Subscriber under test cannot make or receive calls.

– N—Subscriber under test can make or receive calls; test calls are dropped.

Step 2 Define the number of digits for the trunk group and CICs that are under test. The defaults for both are 4.

```
change ca-config::test-trunk-grp-digits=<x>;
change ca-config::test-trunk-member-digits=<x>;
```

Dial Plan

If the nanp-dial-plan token in the Dial Plan Profile table is set to Y, then the nature of address (NOA) in the Dial Plan table cannot be UNKNOWN. The NOA can be set to NATIONAL. The first digit of the prefix cannot be 1—use any number between 2–9.

Sample Configurations

The following sample configurations illustrate how to configure the Cisco BTS 10200 Softswitch for ISDN NLB with network terminating equipment (NTE).

Note In these samples, digit-string=***nnn*** (where nnn = 551 and so forth), ***nnn*** is the test-prefix.

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*.

Line Loopback Tests over an ISDN Trunks

This section provides examples of Network Test Equipment (NTE) line loopback over ISDN trunks.

NLB Tests

This section provides examples of network loopback (NLB) line loopback tests over ISDN trunks.

NLB Line Loopback Test over an ISDN Trunk

This section provides example steps to use the feature for NTE NLB trunk test over an ISDN trunk.

	Perform the Following Command or Action:	Purpose
Step 1	`add destination dest-id=nlb-line-test; call-type=test-call; call-subtype=nlb-line-test;`	Provision the Destination table.
Step 2	`add dial plan id=<xxx>; digit-string=551; dest-id=nlb-trunk-test; split-npa=none; del-digits=0; min-digits=13; max-digits=13; noa=national;` **Note** Where <xxx> is an existing dial plan. The dial plan id must match to the LB test prefix (for example 551) in the digit string.	Provision the Dial Plan table. The digit-string plus the min-digits and max-digits total depends on the settings configured (if any) in the "Call Agent Configuration Table" section.

Then:

1. From the test equipment, dial the NTE NLB trunk test call (551+xxx-xxx-xxxx). The BCM does not notify the Feature Server of this call and the call is looped back.
2. Hang up the test call and verify the Billing call type.

NLB Line Loopback Test over an ISDN Trunk with Service Affecting Turned On

This section provides example steps to use the feature for NTE NLB line test over an ISDN trunk with service affecting turned on.

	Perform the Following Command or Action:	Purpose
Step 1	`add destination dest-id=nlb-line-test; call-type=test-call; call-subtype=nlb-line-test;`	Provision the Destination table.
Step 2	`add dial plan id=<xxx>; digit-string=551; dest-id=nlb-line-test; split-npa=none; del-digits=0; min-digits=13; max-digits=13; noa=national;` **Note** Where <xxx> is an existing dial plan. The dial plan id must match to the LB test prefix (for example 551) in the digit string.	Provision the Dial Plan table. The digit-string plus the min-digits and max-digits total depends on the settings configured (if any) in the "Call Agent Configuration Table" section.
Step 3	`add ca-config type=nlb-test-service-affecting=y; datatype=boolean;value=y;`	Provision the Call Agent Configuration table with service affecting on.

Then:

1. From the test equipment, dial the NTE NLB line test call (551+xxx-xxx-xxxx). The BCM does not notify the Feature Server of this call and the call is looped back.
2. Take the subscriber under test off-hook. There is no dial tone.
3. Call the subscriber under test from another subscriber. Call is treated, and the test call is still active.
4. Hang up the test call and verify the Billing call type.

NLB Line Loopback Test over an ISDN Trunk with Service Affecting Turned Off and Parallel Test Connection Support Turned Off

This section provides example steps to use the feature for NTE NLB line test over an ISDN trunk with service affecting turned off.

	Perform the Following Command or Action:	Purpose
Step 1	`add destination dest-id=nlb-line-test; call-type=test-call; call-subtype=nlb-line-test;`	Provision the Destination table.

	Perform the Following Command or Action:	Purpose
Step 2	`add dial plan id=<xxx>; digit-string=551; dest-id=nlb-line-test; split-npa=none; del-digits=0; min-digits=13; max-digits=13; noa=national;` **Note** Where <xxx> is an existing dial plan. The dial plan id must match to the LB test prefix (for example 551) in the digit string.	Provision the Dial Plan table. The digit-string plus the min-digits and max-digits total depends on the settings configured (if any) in the "Call Agent Configuration Table" section.
Step 3	`add ca-config type=nlb-test-service-affecting=n; datatype=boolean;value=n;`	Provision the Call Agent Configuration table with service affecting off.

Then:

1. From the test equipment, dial the NTE NLB-LINE test call (551+xxx-xxx-xxxx). The BCM does not notify the Feature Server of this call and the call is looped back.
2. Take the subscriber under test off-hook. There is a dial tone.
3. Call the subscriber under test from another subscriber. Call is set up, and the test call is released.
4. Hang up the test call and verify the Billing call type.

NLB Line Loopback Test over an ISDN Trunk with Service Affecting Turned Off and Parallel Test Connection Support Turned On: Call from Subscriber under Test

This section provides example steps to use the feature for NTE NLB line test over an ISDN trunk with service affecting turned on and parallel test connection support turned on; call is from the subscriber under test.

	Perform the Following Command or Action:	Purpose
Step 1	`add destination dest-id=nlb-line-test; call-type=test-call; call-subtype=nlb-line-test;`	Provision the Destination table.
Step 2	`add dial plan id=<xxx>; digit-string=551; dest-id=nlb-line-test; split-npa=none; del-digits=0; min-digits=13; max-digits=13; noa=national;` **Note** Where <xxx> is an existing dial plan. The dial plan id must match to the LB test prefix (for example 551) in the digit string.	Provision the Dial Plan table. The digit-string plus the min-digits and max-digits total depends on the settings configured (if any) in the "Call Agent Configuration Table" section.
Step 3	`add ca-config type=nlb-test-service-affecting=n; datatype=boolean;value=n;`	Provision the Call Agent Configuration table with service affecting off.
Step 4	`change mgw-profile id=isdnNLB; parallel-test-conn-supp=y;`	Turn on support parallel test connection in the Media Gateway Profile table.

Then:

1. From the test equipment, dial the NTE NLB line test call (551+xxx-xxx-xxxx). The BCM does not notify the Feature Server of this call and the call is looped back.
2. Take the subscriber under test off-hook. There is a dial tone.
3. Call the subscriber under test from another subscriber. Call is set up, and the test call is still active.

4. Hang up the test call and verify the Billing call type.

NLB Line Loopback Test over an ISDN Trunk with Service Affecting Turned Off and Parallel Test Connection Support Turned On: Call to Subscriber under Test

This section provides example steps to use the feature for NTE NLB line test over an ISDN trunk with service affecting turned off and parallel test connection support turned on; call is to the subscriber under test.

	Perform the Following Command or Action:	Purpose
Step 1	`add destination dest-id=nlb-line-test; call-type=test-call; call-subtype=nlb-line-test;`	Provision the Destination table.
Step 2	`add dial plan id=<xxx>; digit-string=551; dest-id=nlb-line-test; split-npa=none; del-digits=0; min-digits=13; max-digits=13; noa=national;` **Note** Where <xxx> is an existing dial plan. The dial plan id must match to the LB test prefix (for example 551) in the digit string.	Provision the Dial Plan table. The digit-string plus the min-digits and max-digits total depends on the settings configured (if any) in the "Call Agent Configuration Table" section.
Step 3	`add ca-config type=nlb-test-service-affecting=n; datatype=boolean;value=n;`	Provision the Call Agent Configuration table with service affecting off.
Step 4	`change mgw-profile id=isdnNLB; parallel-test-conn-supp=y;`	Turn on support parallel test connection in the Media Gateway Profile table.

Then:

1. From the test equipment, dial the NTE NLB-LINE test call (551+xxx-xxx-xxxx). The BCM does not notify the Feature Server of this call and the call is looped back.
2. Take the subscriber under test off-hook. There is a dial tone.
3. Call the subscriber under test from another subscriber. Call is set up, and the test call stays up.
4. Verify the Billing call type.

NCT Tests

This section provides examples of line loopback network continuity tests (NCT) over ISDN.

NCT Line Loopback Test over an ISDN Trunk

This section provides example steps to use the feature for NTE NLB trunk test over an ISDN trunk.

	Perform the Following Command or Action:	Purpose
Step 1	`add destination dest-id=nlb-line-test; call-type=test-call; call-subtype=nct-line-test;`	Provision the Destination table.
Step 2	`add dial plan id=<xxx>; digit-string=552; dest-id=nlb-trunk-test; split-npa=none; del-digits=0; min-digits=13; max-digits=13; noa=national;` **Note** Where <xxx> is an existing dial plan. The dial plan id must match to the LB test prefix (for example 552) in the digit string.	Provision the Dial Plan table. The digit-string plus the min-digits and max-digits total depends on the settings configured (if any) in the "Call Agent Configuration Table" section.

Then:

1. From the test equipment, dial the NTE NLB trunk test call (552+xxx-xxx-xxxx). The BCM does not notify the Feature Server of this call and the call is looped back.
2. Hang up the test call and verify the Billing call type.

NCT Line Loopback Test over an ISDN Trunk with Service Affecting Turned On

This section provides example steps to use the feature for NTE NCT line test over an ISDN trunk with service affecting turned on.

	Perform the Following Command or Action:	Purpose
Step 1	`add destination dest-id=nlb-line-test; call-type=test-call; call-subtype=nct-line-test;`	Provision the Destination table.
Step 2	`add dial plan id=<xxx>; digit-string=552; dest-id=nlb-line-test; split-npa=none; del-digits=0; min-digits=13; max-digits=13; noa=national;` **Note** Where <xxx> is an existing dial plan. The dial plan id must match to the LB test prefix (for example 552) in the digit string.	Provision the Dial Plan table. The digit-string plus the min-digits and max-digits total depends on the settings configured (if any) in the "Call Agent Configuration Table" section.
Step 3	`add ca-config type=nlb-test-service-affecting=y; datatype=boolean;value=y;`	Provision the Call Agent Configuration table with service affecting on.

Then:

1. From the test equipment, dial the NTE NLB line test call (552+xxx-xxx-xxxx). The BCM does not notify the Feature Server of this call and the call is looped back.
2. Take the subscriber under test off-hook. There is no dial tone.
3. Call the subscriber under test from another subscriber. Call is treated, and the test call is still active.
4. Hang up the test call and verify the Billing call type.

NCT Line Loopback Test over an ISDN Trunk with Service Affecting Turned Off and Parallel Test Connection Support Turned Off

This section provides example steps to use the feature for NTE NCT line test over an ISDN trunk with service affecting turned off.

	Perform the Following Command or Action:	Purpose
Step 1	`add destination dest-id=nlb-line-test; call-type=test-call; call-subtype=nct-line-test;`	Provision the Destination table.
Step 2	`add dial plan id=<xxx>; digit-string=552; dest-id=nlb-line-test; split-npa=none; del-digits=0; min-digits=13; max-digits=13; noa=national;` **Note** Where <xxx> is an existing dial plan. The dial plan id must match to the LB test prefix (for example 552) in the digit string.	Provision the Dial Plan table. The digit-string plus the min-digits and max-digits total depends on the settings configured (if any) in the "Call Agent Configuration Table" section.
Step 3	`add ca-config type=nlb-test-service-affecting=n; datatype=boolean;value=n;`	Provision the Call Agent Configuration table with service affecting off.

Then:

1. From the test equipment, dial the NTE NLB-LINE test call (552+xxx-xxx-xxxx). The BCM does not notify the Feature Server of this call and the call is looped back.
2. Take the subscriber under test off-hook. There is a dial tone.
3. Call the subscriber under test from another subscriber. Call is set up, and the test call is released.
4. Hang up the test call and verify the Billing call type.

NCT Line Loopback Test over an ISDN Trunk with Service Affecting Turned Off and Parallel Test Connection Support Turned On: Call from Subscriber under Test

This section provides example steps to use the NTE NCT line test over an ISDN trunk with service affecting turned on and parallel test connection support turned on; call is from the subscriber under test.

	Perform the Following Command or Action:	Purpose
Step 1	`add destination dest-id=nlb-line-test; call-type=test-call; call-subtype=nct-line-test;`	Provision the Destination table.
Step 2	`add dial plan id=<xxx>; digit-string=552; dest-id=nlb-line-test; split-npa=none; del-digits=0; min-digits=13; max-digits=13; noa=national;` **Note** Where <xxx> is an existing dial plan. The dial plan id must match to the LB test prefix (for example 552) in the digit string.	Provision the Dial Plan table. The digit-string plus the min-digits and max-digits total depends on the settings configured (if any) in the "Call Agent Configuration Table" section.
Step 3	`add ca-config type=nlb-test-service-affecting=n; datatype=boolean;value=n;`	Provision the Call Agent Configuration table with service affecting off.
Step 4	`change mgw-profile id=isdnNLB; parallel-test-conn-supp=y;`	Turn on support parallel test connection in the Media Gateway Profile table.

Then:

1. From the test equipment, dial the NTE NLB line test call (552+xxx-xxx-xxxx). The BCM does not notify the Feature Server of this call and the call is looped back.
2. Take the subscriber under test off-hook. There is a dial tone.

3. Call the subscriber under test from another subscriber. Call is set up, and the test call is still active.
4. Hang up the test call and verify the Billing call type.

NCT Line Loopback Test over an ISDN Trunk with Service Affecting Turned Off and Parallel Test Connection Support Turned On: Call to Subscriber under Test

This section provides example steps to use the feature for NTE NCT line test over an ISDN trunk with service affecting turned off and parallel test connection support turned on; call is to the subscriber under test.

	Perform the Following Command or Action:	Purpose
Step 1	`add destination dest-id=nlb-line-test; call-type=test-call; call-subtype=nct-line-test;`	Provision the Destination table.
Step 2	`add dial plan id=<xxx>; digit-string=552; dest-id=nlb-line-test; split-npa=none; del-digits=0; min-digits=13; max-digits=13; noa=national;` **Note** Where <xxx> is an existing dial plan. The dial plan id must match to the LB test prefix (for example 552) in the digit string.	Provision the Dial Plan table. The digit-string plus the min-digits and max-digits total depends on the settings configured (if any) in the "Call Agent Configuration Table" section.
Step 3	`add ca-config type=nlb-test-service-affecting=n; datatype=boolean;value=n;`	Provision the Call Agent Configuration table with service affecting off.
Step 4	`change mgw-profile id=isdnNLB; parallel-test-conn-supp=y;`	Turn on support parallel test connection in the Media Gateway Profile table.

Then:

1. From the test equipment, dial the NTE NLB-LINE test call (552+xxx-xxx-xxxx). The BCM does not notify the Feature Server of this call and the call is looped back.
2. Take the subscriber under test off-hook. There is a dial tone.
3. Call the subscriber under test from another subscriber. Call is set up, and the test call stays up.

Verify the Billing call type.

Trunk Loopback Tests over an ISDN Trunk

For trunk loopback testing when the test call and normal call are on the same circuit, the normal call always has precedence. For example:

1. if the test call is on circuit *xxx* and a normal call comes in on the same circuit, then the normal call is set up and the test call is released.
2. if a normal call is on circuit *xxx* and a test call comes in on same circuit, then the normal call stays up and the test call is released.

NLB Trunk Loopback Test over an ISDN Trunk

This section provides example steps to use the feature for an NTE NLB trunk test over an ISDN trunk.

	Perform the Following Command or Action:	Purpose
Step 1	`add destination dest-id=nlb-trunk-test; call-type=test-call; call-subtype=nlb-trunk-test;`	Provision the Destination table.
Step 2	`add dial plan id=<xxx>; digit-string=553; dest-id=nlb-trunk-test; split-npa=none; del-digits=0; min-digits=11; max-digits=11; noa=national;` **Note** Where <xxx> is an existing dial plan. The dial plan id must match to the LB test prefix (for example 553) in the digit string.	Provision the Dial Plan table. The digit-string plus the min-digits and max-digits total depends on the settings configured (if any) in the "Call Agent Configuration Table" section.

Then:

1. From the test equipment, dial the NTE NLB trunk test call (553+trunk digits+members).
2. Hang up the test call and verify the Billing call type.

NCT Trunk Loopback Test over an ISDN Trunk

This section provides example steps to use the feature for an NTE NLB trunk test over an ISDN trunk.

	Perform the Following Command or Action:	Purpose
Step 1	`add destination dest-id=nct-trunk-test; call-type=test-call; call-subtype=nct-trunk-test;`	Provision the Destination table.
Step 2	`add dial plan id=<xxx>; digit-string=554; dest-id=nlb-trunk-test; split-npa=none; del-digits=0; min-digits=11; max-digits=11; noa=national;` **Note** Where <xxx> is an existing dial plan. The dial plan id must match to the LB test prefix (for example 554) in the digit string.	Provision the Dial Plan table. The digit-string plus the min-digits and max-digits total depends on the settings configured (if any) in the "Call Agent Configuration Table" section.
Step 3	`add trunk-grp id=nte; call-agent-id=CA146; tg-type=isdn; dial-plan-id=nte; dpc=101-55-103; tg-profile-id=ISDN1;call-ctrl-route-id=ccr1;`	Provision the Trunk Group table.

Then:

1. From the test equipment, dial the NTE NLB trunk test call (554+trunk digits+members) (trunk)
2. Hang up the test call and verify the Billing call type.

Enhanced Traffic Measurement

The Cisco BTS 10200 supports both traditional PSTN measurements as well as additional requirements required by the IP and ATM backbones that the services are offered over. Many of the informational elements within the measurement data find their basis in the traditional PSTN TDM network implementations with modifications and additions caused by the expanded needs and capabilities of the converged network environment. The Cisco BTS 10200 measurement information includes both

statistical and performance details. The mechanism used to manage the data generated and transported from the Cisco BTS 10200 system follows legacy type procedures and are documented in the following sections.

Measurement Data Transport and Access

The measurement data collected on the Cisco BTS 10200 can be accessed through several different mechanisms. The Command Line Interface, which runs over a telnet or SSH session, is used in the examples within this document. Measurement data is also available in CSV or XML format through the FTP or SFTP interface. The measurement data can be provisioned and is accessible through the SNMP MIB. The supported version of SNMP on the Cisco BTS 10200 is v2c. There is detailed information on both of these access mechanisms available in separate operations manuals.

Measurement Data Event Reports

The measurement subsystem within the BTS 10200 supports several events that are issued in various abnormal scenarios. Table 15-5 illustrates the event reports that the measurements subsystem supports and their significance.

Table 15-5 Event Reports Supported by Measurement Subsystem

Type and Number	Severity	Description	Meaning
STATISTICS (2)	Informational	Call Agent Measurement Collection Started	Issued whenever the traffic process running on the call agent platform begins a new collection cycle for the current interval.
STATISTICS (3)	Informational	Call Agent Measurement Collection Finished	Issued whenever the traffic process running on the call agent platform completes a collection cycle for the current interval.
STATISTICS (4)	Informational	POTS/CTX/TDM Measurement Collection Started	Issued whenever the traffic process running on the POTS Feature Server platform begins a new collection cycle for the current interval.
STATISTICS (5)	Informational	POTS/CTX/TDM Measurement Collection Finished	Issued whenever the traffic process running on the POTS Feature Server platform completes a collection cycle for the current interval.
STATISTICS (6)	Informational	AIN Measurement Collection Started	Issued whenever the traffic process running on the AIN Feature Server platform begins a new collection cycle for the current interval.
STATISTICS (7)	Informational	AIN Measurement Collection Finished	Issued whenever the traffic process running on the AIN Feature Server platform completes a collection cycle for the current interval.
STATISTICS (8)	Warning	Message Send Failure	Issued whenever the traffic manager process in the EMS or the traffic agent process in any element is unable to send an inter-process message

Table 15-5 Event Reports Supported by Measurement Subsystem (continued)

Type and Number	Severity	Description	Meaning
STATISTICS (9)	Warning	Measurement Table SQL Read Error	Issued whenever the traffic manager process in the EMS is unable to read from one of the measurement tables stored in Oracle
STATISTICS (10)	Warning	Measurement Table SQL Write Error	Issued whenever the traffic manager process in the EMS is unable to write to one of the measurement tables stored in Oracle
STATISTICS (11)	Warning	Measurement Collection API Failure	Issued whenever the traffic agent process in any of the BTS 10200 elements is unable to access the counter stored within shared memory via the standard API invocations
STATISTICS (12)	Major	Schemas out of Synchronization	Issued whenever system detects a mismatch between the counter schema in Oracle on the BDMS and the internal schema of the call agents and/or feature servers
STATISTICS (13)	Major	TMM API Failure	Issued whenever the TMM collection process is unable to initialize or attach to shared memory

Operating

The following sections provide detailed information on how to manage and control the measurement information generated by the Cisco BTS 10200 system. Actual examples are provided with explanations to illustrate the operational mechanics. These and other commands are documented in the Cisco BTS 10200 Softswitch Command Line Interface Reference Manual and the Cisco BTS 10200 Softswitch Operations and Maintenance Guide.

Provisioning Measurement Report Types

The BTS 10200 system provides a command line interface to manage the collection of the measurement information generated. This mechanism provides the ability to enable or disable the collection of measurement data and specify the reporting interval on a per report type basis. The factory default setting is to enable the collection of all measurement types and to set the reporting intervals to 15 minutes. Currently, there are 13 types of measurement data generated by the Cisco BTS 10200. The following list illustrates each of these categories of data:

- ISDN - ISDN signaling protocol related information
- CALLP - Call Processing specific information
- MGCP - MGCP signaling protocol related information
- SIM - Service Interaction Manager related information
- POTS-SVC - POTS/Centrex/Tandem Feature Service related information
  - POTS-LOCAL - Local Feature counters
  - POTS-MISC - Miscellaneous Feature counters
  - POTS-SLE - Screening List Editing counters

  - POTS-ACAR - Auto Callback / Recall counters
  - POTS-COS - Class Of Service counters
  - POTS-COT - Customer Originated Trace counters
- AINSVC - AIN Feature Service related information
- ISUP - ISDN User Part (SS7) signaling protocol related information - in a Signaling Gateway configuration
- AUDIT - Auditing related information
- SIA - SIP Interface Adapter related information
- BILLING - Call Detail Data related information
- EM - Event Messaging Billing related information
- DQOS - Dynamic Quality of Service related information
- SNMP - SNMP agent protocol related information
- TG-USG - Trunk Group usage information
- ANM - Announcement server related information
- H323 - H.323 signaling protocol related information
- M3UA - M3UA signaling protocol related information
- SUA - SUA signaling protocol related information
- SCTP - SCTP signaling protocol related information
- SCCP - SCCP protocol related information
- TCAP - TCAP related protocol information
- CALL-TOOLS - Metrics related to invocations of the Translation Verification Tools
- AIN-TOOLS - Metrics related to invocations of the Toll Free and LNP Query Verification Tools
- PCT-TOOLS - Metrics related to invocations of the LIDB Query Verification Tools
- ALL - All categories of measurements available on the BTS 10200

The following is an example of the command line used to provision the collection of the call processing measurement data:

```
change measurement-prov type=callp; enable=yes; time-interval=15;
```

The following is a list of the command line tokens associated with this command and the valid values and purpose of each:

- Type—An ASCII character string from 3 to 8 inches long. The string must match one of the types listed above. This is a mandatory token.
- Enable—An ASCII character string of Yes or No. This string specifies whether or not to perform collection on the specified measurement type. This is an optional token that is pre-provisioned with a value of YES at the factory. Either this token and/or the time-interval token must be entered
- Time-interval—A decimal value of 5, 15, 30, or 60. This value indicates the number of minutes each reporting interval is to encompass for the given report type. The reporting interval is always synchronized to zero minutes after the hour for consistency. This is an optional token that is pre-provisioned with a value of 15 at the factory. Changing this value does not take effect until the completion of the current collection interval based on the previous time-interval setting. Either this token and/or the enable token must be entered.

The following are examples of the command line invocations to display the current settings for the data described above:

```
show measurement-prov type=callp;

show measurement-prov type=anm;

show measurement-prov type=isdn;

show measurement-prov type=billing;

show measurement-prov type=em;

show measurement-prov type=snmp;

show measurement-prov type=mgcp;

show measurement-prov type=sim;

show measurement-prov type=pots-fs;

show measurement-prov type=ainsvc;

show measurement-prov type=tcap;

show measurement-prov type=m3ua;

show measurement-prov type=sua;

show measurement-prov type=sctp;

show measurement-prov type=sccp;

show measurement-prov type=isup;

show measurement-prov type=audit;

show measurement-prov type=sia;

show measurement-prov type=dqos;

show measurement-prov type=tg-usg;

show measurement-prov type=h323;

show measurement-prov type=call-tools;

show measurement-prov type=ain-tools;

show measurement-prov type=pct-tools;
```

Measurement Report Summaries

The Cisco BTS 10200 system provides a command line interface (CLI) command to query summary reports of measurement data from the database on the Element Management System (EMS). This mechanism provides the ability to specify an interval and the particular type and source of data. The time interval specified must be prior to the current collection interval.

The following are examples of the command line queries to generate reports on the various types of measurements collected from the designated call agents and feature servers from 10 am until noon on March 27th, 2002 and places the data into CSV files for FTP.

Note Any measurement counters that do not contain data for a given interval are suppressed out of the reports generated. Only counters that were pegged are presented in the resulting summaries.

```
report measurement-isdn-summary start-time=2002-03-27 10:00:00; end-time=2002-03-27
12:00:00; call-agent-id=CA146; output=isdn-report; output-type=csv;

report measurement-callp-summary start-time=2002-03-27 10:00:00; end-time=2002-03-27
12:00:00; call-agent-id= CA146; output=callp-report; output-type=csv;

report measurement-mgcp-summary start-time=2002-03-27 10:00:00; end-time=2002-03-27
12:00:00; call-agent-id= CA146; output=mgcp-report; output-type=csv;

report measurement-sim-summary start-time=2002-03-27 10:00:00; end-time=2002-03-27
12:00:00; call-agent-id= CA146; output=sim-report; output-type=csv;

report measurement-pots-local-summary start-time=2002-03-27 10:00:00; end-time=2002-03-27
12:00:00; feature-server-id=PCT01; output=pots-local-report; output-type=csv;

report measurement-pots-misc-summary start-time=2002-03-27 10:00:00; end-time=2002-03-27
12:00:00; feature-server-id=PCT01; output=pots-misc-report; output-type=csv;

report measurement-pots-sle-summary start-time=2002-03-27 10:00:00; end-time=2002-03-27
12:00:00; feature-server-id=PCT01; output=pots-sle-report; output-type=csv;

report measurement-pots-acar-summary start-time=2002-03-27 10:00:00; end-time=2002-03-27
12:00:00; feature-server-id=PCT01; output=pots-acar-report; output-type=csv;

report measurement-pots-cos-summary start-time=2002-03-27 10:00:00; end-time=2002-03-27
12:00:00; feature-server-id=PCT01; output=pots-cos-report; output-type=csv;

report measurement-pots-cot-summary start-time=2002-03-27 10:00:00; end-time=2002-03-27
12:00:00; feature-server-id=PCT01; output=pots-cot-report; output-type=csv;

report measurement-ainsvc-summary start-time=2002-03-27 10:00:00; end-time=2002-03-27
12:00:00; feature-server-id=AIN01; output=ainsvc-report; output-type=csv;

report measurement-sccp-summary start-time=2002-03-27 10:00:00; end-time=2002-03-27
12:00:00; feature-server-id=AIN01; output=sccp-report; output-type=csv;

report measurement-tcap-summary start-time=2002-03-27 10:00:00; end-time=2002-03-27
12:00:00; feature-server-id=AIN01; output=tcap-report; output-type=csv;

report measurement-m3ua-summary start-time=2002-03-27 10:00:00; end-time=2002-03-27
12:00:00; sgp-id=sg-001; output=m3ua-report; output-type=csv;

report measurement-sua-summary start-time=2002-03-27 10:00:00; end-time=2002-03-27
12:00:00; sgp-id=sg-001; output=sua-report; output-type=csv;

report measurement-sctp-summary start-time=2002-03-27 10:00:00; end-time=2002-03-27
12:00:00; sctp-assoc-id=assoc-001; output=sctp-report; output-type=csv;

report measurement-isup-summary start-time=2002-03-27 10:00:00; end-time=2002-03-27
12:00:00; tgn-id=dallas01; output=isup-report; output-type=csv;

report measurement-audit-summary start-time=2002-03-27 10:00:00; end-time=2002-03-27
12:00:00; call-agent-id= CA146; output=audit-report; output-type=csv;

report measurement-sia-summary start-time=2002-03-27 10:00:00; end-time=2002-03-27
12:00:00; call-agent-id= CA146; output=sia-report; output-type=csv;
```

```
report measurement-billing-summary start-time=2002-03-27 10:00:00; end-time=2002-03-27
12:00:00; call-agent-id= CA146; output=billing-report; output-type=csv;

report measurement-em-summary start-time=2002-03-27 10:00:00; end-time=2002-03-27
12:00:00; call-agent-id= CA146; output=em-report; output-type=csv;

report measurement-dqos-summary start-time=2002-03-27 10:00:00; end-time=2002-03-27
12:00:00; aggr-id=AGGR01; output=dqos-report; output-type=csv;

report measurement-snmp-summary start-time=2002-03-27 10:00:00; end-time=2002-03-27
12:00:00; output=snmp-report; output-type=csv;

report measurement-tg-usage-summary start-time=2002-03-27 10:00:00; end-time=2002-03-27
12:00:00; tgn-id=dallas01; call-agent-id=CA146; output=tg-report; output-type=csv;

report measurement-tg-usage-summary start-time=2002-03-27 10:00:00; end-time=2002-03-27
12:00:00; trkgrp-exchange= RONLVA31GT; trkgrp-name= RONKVACSDS0_LC; call-agent-id=CA146;
output=tg-report; output-type=csv;  (this is a new reporting option to gather statistics
on a per Pop basis)

report measurement-anm-summary start-time=2002-03-27 10:00:00; end-time=2002-03-27
12:00:00; call-agent-id= CA146; output=anm-report; output-type=csv;

report measurement-h323-summary start-time=2002-03-27 10:00:00; end-time=2002-03-27
12:00:00; call-agent-id= CA146; output=h323-report; output-type=csv;

report measurement-call-tools-summary start-time=2002-03-27 10:00:00; end-time=2002-03-27
12:00:00; call-agent-id=CA146; output=call-tools-report; output-type=csv;

report measurement-ain-tools-summary start-time=2002-03-27 10:00:00; end-time=2002-03-27
12:00:00; feature-server-id=AIN01; output=ain-tools-report; output-type=csv;

report measurement-pct-tools-summary start-time=2002-03-27 10:00:00; end-time=2002-03-27
12:00:00; feature-server-id=PCT01; output=pct-tools-report; output-type=csv;
```

Command Line Tokens

The following table lists the command line tokens associated with this command and the valid values and purpose of each:

Table 15-6 Command Line Tokens Associated with Measurement Report Summaries

Command Line Token	Description
start-time	A time stamp value in the format of YYYY-MM-DD HH:MM:SS. This value indicates the starting interval time to search for within the EMS database. This is an optional token. When omitted, it results in the display of the last collected interval.
end-time	A time stamp value in the format of YYYY-MM-DD HH:MM:SS. This value indicates the stopping interval time to search for within the EMS database. This is an optional token. When omitted, it results in the display of the last collected interval.

Table 15-6 Command Line Tokens Associated with Measurement Report Summaries (continued)

Command Line Token	Description
interval	This token is optional and is used to specify that a report be generated that contains counter information for the interval currently under collection (CURRENT) or all of the collected intervals persisted on disk (ALL). If this token is used on the command line, it overrides start-time and end-time tokens that are specified. If entered, the corresponding call-agent-id or feature-server-id must be specified. There is no default value for this token. If this token **and** the start-time token are not entered by the user, the last collected interval is reported.
sum	This token indicates whether the resulting report request contains the individual interval reports (N) or a summation of all interval reports into one composite report (Y). The default value for this token is N. This token is not allowed in combination with the trunk group category.
output	This token indicates the name of the file to be created and the location where the resulting measurement data is placed. The file name is pre-pended with the string "Tm_" and placed in the /opt/ems/report directory on the active EMS.
output-type	The format of the output file, which can be in comma-separated value (csv) or XML format.
display	Allows you to specify the columns of data to present in the resulting report. Only those columns specified are shown in the report. If you enter a value of "%", then a list of all possible column values are displayed, but the report itself is not created.
call-agent-id	The identity of the call agent that collected the measurement data. This is an optional token that defaults to all call agents and is only applicable to the following measurement types: • call-tools • billing • callp • mgcp • isdn • audit • sia • sim • anm • h323 • tg-usage • em

Table 15-6 Command Line Tokens Associated with Measurement Report Summaries (continued)

Command Line Token	Description
feature-server-id	The identity of the feature server that collected the measurement data. This is an optional token that defaults to all feature servers and is only applicable to the following measurement types: • pct-tools • ain-tools • ainsvc • sccp • tcap • pots-local • pots-misc • pots-sle • pots-acar • pots-cos • pots-cot
tgn-id	The trunk group numbers used to report measurement data. This is an optional token that is only applicable to the following measurement types: • tg-usage • isup When used with the trunk measurement type, it results in all trunks within the trunk group being reported.
sgp-id	The signaling gateway process for reporting measurement data. This is an optional token that is only applicable to the following measurement types: • m3ua • sua
sctp-assoc-id	The sctp association id for reporting measurement data. This is an optional token that is only applicable to the following measurement type: • sctp
aggr-id	The aggregation id for reporting measurement data. This is an optional token that is only applicable to the following measurement type: • dqos

Reporting Current Interval Counts

The BTS 10200 system provides a CLI command to query in-progress partial interval counts of measurement data from the actual source of the data. This mechanism provides the ability to specify the current collection interval and the particular type and source of data. The start time specified must fall within the current collection interval.

Note This command is not supported for trunk and tg-usage measurement types.

The following are examples of the command line queries to generate reports on the various types of measurements currently being collected from call agents and feature servers on March 27th, 2002 assuming the time is presently 10:05 in the morning:

```
report measurement-isdn-summary call-agent-id=CA146; output=isdn-partial-report;
interval=current; output-type=csv;

report measurement-callp-summary call-agent-id= CA146; output=callp-partial-report;
interval=current; output-type=csv;

report measurement-mgcp-summary call-agent-id= CA146; output=mgcp-partial-report;
interval=current; output-type=csv;

report measurement-sim-summary call-agent-id= CA146; output=sim-partial-report;
interval=current; output-type=csv;

report measurement-pots-local-summary feature-server-id=PCT01;
output=pots-local-partial-report; interval=current; output-type=csv;

report measurement-pots-misc-summary feature-server-id=PCT01;
output=pots-misc-partial-report; interval=current; output-type=csv;

report measurement-pots-sle-summary feature-server-id=PCT01;
output=pots-sle-partial-report; interval=current; output-type=csv;

report measurement-pots-acar-summary feature-server-id=PCT01;
output=pots-acar-partial-report; interval=current; output-type=csv;

report measurement-pots-cos-summary feature-server-id=PCT01;
output=pots-cos-partial-report; interval=current; output-type=csv;

report measurement-pots-cot-summary feature-server-id=PCT01;
output=pots-cot-partial-report; interval=current; output-type=csv;

report measurement-ainsvc-summary call-agent-id=AIN01; output=ainsvc-partial-report;
interval=current; output-type=csv;

report measurement-sccp-summary call-agent-id=AIN01; output=sccp-partial-report;
interval=current; output-type=csv;

report measurement-tcap-summary call-agent-id=AIN01; output=tcap-partial-report;
interval=current; output-type=csv;

report measurement-audit-summary call-agent-id=CA146; output=audit-partial-report;
interval=current; output-type=csv;

report measurement-sia-summary call-agent-id=CA146; output=sia-partial-report;
interval=current; output-type=csv;

report measurement-billing-summary call-agent-id=CA146; output=billing-partial-report;
interval=current; output-type=csv;

report measurement-em-summary call-agent-id=CA146; output=em-partial-report;
interval=current; output-type=csv;

report measurement-snmp-summary output=snmp-partial-report; interval=current;
output-type=csv;
```

```
report measurement-anm-summary call-agent-id=CA146; output=anm-partial-report;
interval=current; output-type=csv;

report measurement-h323-summary call-agent-id=CA146; output=h323-partial-report;
interval=current; output-type=csv;

report measurement-call-tools-summary call-agent-id=CA146;
output=call-tools-partial-report; interval=current; output-type=csv;

report measurement-ain-tools-summary feature-server-id=AIN01;
output=ain-tools-partial-report; interval=current; output-type=csv;

report measurement-pct-tools-summary feature-server-id=PCT01;
output=pct-tools-partial-report; interval=current; output-type=csv;
```

The following table lists the command line tokens associated with this command and the valid values and purpose of each:

Table 15-7 Command Line Tokens Associated with Reporting Current Interval Counts

Command Line Token	Description
start-time	A time stamp value with the format of YYYY-MM-DD HH:MM:SS. This value indicates the starting interval time to search for within the EMS database. This is a mandatory token.
output	The name of the file to be created and location to place the resulting measurement data. The file name is pre-pended with the string "Tm_" and placed in the /opt/ems/report directory on the active EMS.
output-type	The format of the output file—it can be in comma-separated value (csv) or XML format.
call-agent-id	The identity of the call agent that collected the measurement data. This is an optional token that defaults to all call agents and is only applicable to the following measurement types: • call-tools • billing • callp • mgcp • isdn • audit • sia • sim • anm • h323 • em

Table 15-7 Command Line Tokens Associated with Reporting Current Interval Counts (continued)

Command Line Token	Description
feature-server-id	The identity of the feature server that collected the measurement data. This is an optional token that defaults to all feature servers and is only applicable to the following measurement types: • ain-tools • pct-tools • ainsvc • sccp • tcap • pots-local • pots-misc • pots-sle • pots-acar • pots-cos • pots-cot
interval	This token is optional and is used to specify that a report be generated that contains counter information for the interval currently under collection (CURRENT) or all of the collected intervals persisted on disk (ALL). If this token is used on the command line, it will override start-time and end-time tokens if they are specified. If entered, the corresponding call-agent-id or feature-server-id must be specified. There is no default value for this token. If this token **and** the start-time token are not entered by the user, the last collected interval is reported.

Clearing Current Interval Counts

The Cisco BTS 10200 system provides a CLI command to clear in-progress partial counts of measurement data at the actual source of the data. This mechanism provides the ability to specify the particular type and source of data.

Caution ***This is a destructive command that will erase the partial counts for the current interval permanently.*** Use this command with caution.

The following examples clear all of the currently accumulating counters in call agents and feature servers:

```
clear measurement-isdn-summary call-agent-id=CA146;

clear measurement-callp-summary call-agent-id=CA146;

clear measurement-mgcp-summary call-agent-id=CA146;

clear measurement-sim-summary call-agent-id=CA146;

clear measurement-pots-local-summary feature-server-id=PCT01;
```

```
clear measurement-pots-misc-summary feature-server-id=PCT01;

clear measurement-pots-sle-summary feature-server-id=PCT01;

clear measurement-pots-acar-summary feature-server-id=PCT01;

clear measurement-pots-cos-summary feature-server-id=PCT01;

clear measurement-pots-cot-summary feature-server-id=PCT01;

clear measurement-ainsvc-summary feature-server-id=AIN01;

clear measurement-sccp-summary feature-server-id=AIN01;

clear measurement-sccp-summary feature-server-id=AIN01;

clear measurement-tcap-summary feature-server-id=AIN01;

clear measurement-audit-summary call-agent-id=CA146;

clear measurement-sia-summary call-agent-id=CA146;

clear measurement-billing-summary call-agent-id=CA146;

clear measurement-em-summary call-agent-id=CA146;

clear measurement-snmp-summary

clear measurement-anm-summary call-agent-id=CA146;

clear measurement-h323-summary call-agent-id=CA146;

clear measurement-call-tools-summary call-agent-id=CA146;

clear measurement-ain-tools-summary feature-server-id=AIN01;

clear measurement-pct-tools-summary feature-server-id=PCT01;
```

The following is a list of the command line tokens associated with this command and the valid values and purpose of each:

Table 15-8 Command Line Tokens Associated with Clearing Current Interval Counts

Command Line Token	Description
call-agent-id	The identity of the call agent that collected the measurement data. This is an optional token that defaults to all call agents and is only applicable to the following measurement types: • call-tools • billing • callp • mgcp • isdn • audit • sia • sim • anm • H.323 • m3ua • em • sctp
feature-server-id	The identity of the feature server that collected the measurement data. This is an optional token that defaults to all feature servers and is only applicable to the following measurement types: • ain-tools • pct-tools • ainsvc • sccp • tcap • m3ua • sctp • pots-local • pots-misc • pots-sle • pots-acar • pots-cos • pots-cot

Measurements

This section provides detailed information on which counters are maintained within each measurement area. A description of the meaning of each counter is also provided. The name of each counter is an exact ASCII match to the label that is printed within the reports issued by the Cisco BTS 10200. These labels can then be used for automation purposes in testing and retrieving data from the BTS 10200 via the command line or FTP interfaces.

ISDN Protocol Counters

Table 15-9 identifies the ISDN protocol counters provided in Release 4.5.

Table 15-9 ISDN Protocol Counters

Counter Label	Counter Context
ISDN_SETUP_TX	The number of ISDN SETUP messages sent from the reporting call agent
ISDN_SETUP_RX	The number of ISDN SETUP messages received by the reporting call agent
ISDN_SETUP_ACK_TX	The number of ISDN SETUP ACK messages sent from the reporting call agent. This counter is not pegged in this release, but is retained for use in a future release.
ISDN_SETUP_ACK_RX	The number of ISDN SETUP ACK messages received by the reporting call agent. This counter is not pegged in this release, but is retained for use in a future release.
ISDN_CALL_PROCEED_TX	The number of ISDN CALL PROCEED messages sent from the reporting call agent
ISDN_CALL_PROCEED_RX	The number of ISDN CALL PROCEED messages received by the reporting call agent
ISDN_ALERTING_TX	The number of ISDN ALERTING messages sent from the reporting call agent
ISDN_ALERTING_RX	The number of ISDN ALERTING messages received by the reporting call agent
ISDN_PROGRESS_TX	The number of ISDN PROGRESS messages sent from the reporting call agent
ISDN_PROGRESS_RX	The number of ISDN PROGRESS messages received by the reporting call agent
ISDN_CONNECT_TX	The number of ISDN CONNECT messages sent from the reporting call agent
ISDN_CONNECT_RX	The number of ISDN CONNECT messages received by the reporting call agent
ISDN_CONNECT_ACK_TX	The number of ISDN CONNECT ACK messages sent from the reporting call agent
ISDN_CONNECT_ACK_RX	The number of ISDN CONNECT ACK messages received by the reporting call agent
ISDN_DISCONNECT_TX	The number of ISDN DISCONNECT messages sent from the reporting call agent
ISDN_DISCONNECT_RX	The number of ISDN DISCONNECT messages received by the reporting call agent
ISDN_RELEASE_TX	The number of ISDN RELEASE messages sent from the reporting call agent
ISDN_RELEASE_RX	The number of ISDN RELEASE messages received by the reporting call agent
ISDN_RELEASE_COMPLETE_TX	The number of ISDN RELEASE COMPLETE messages sent from the reporting call agent
ISDN_RELEASE_COMPLETE_RX	The number of ISDN RELEASE COMPLETE messages received by the reporting call agent
ISDN_RESTART_TX	The number of ISDN RESTART messages sent from the reporting call agent
ISDN_RESTART_RX	The number of ISDN RESTART messages received by the reporting call agent
ISDN_RESTART_ACK_TX	The number of ISDN RESTART ACK messages sent from the reporting call agent
ISDN_RESTART_ACK_RX	The number of ISDN RESTART ACK messages received by the reporting call agent

Table 15-9 ISDN Protocol Counters (continued)

Counter Label	Counter Context
ISDN_INFORMATION_TX	The number of ISDN INFORMATION messages sent from the reporting call agent
ISDN_INFORMATION_RX	The number of ISDN INFORMATION messages received by the reporting call agent
ISDN_NOTIFY_TX	The number of ISDN NOTIFY messages sent from the reporting call agent
ISDN_NOTIFY_RX	The number of ISDN NOTIFY messages received by the reporting call agent
ISDN_STATUS_TX	The number of ISDN STATUS messages sent from the reporting call agent
ISDN_STATUS_RX	The number of ISDN STATUS messages received by the reporting call agent
ISDN_STATUS_ENQUIRY_TX	The number of ISDN STATUS ENQUIRY messages sent from the reporting call agent
ISDN_STATUS_ENQUIRY_RX	The number of ISDN STATUS ENQUIRY messages received by the reporting call agent
ISDN_SRVC_TX	The number of ISDN SERVICE messages sent from the reporting call agent
ISDN_SRVC_RX	The number of ISDN SERVICE messages received by the reporting call agent
ISDN_SRVC_ACK_TX	The number of ISDN SERVICE ACK messages sent from the reporting call agent
ISDN_SRVC_ACK_RX	The number of ISDN SERVICE ACK messages received by the reporting call agent
ISDN_FACILITY_TX	The number of ISDN FACILITY messages sent from the reporting call agent
ISDN_FACILITY_RX	The number of ISDN FACILITY messages received by the reporting call agent
ISDN_SUSPEND_TX	The number of ISDN Suspend messages sent from the reporting call agent. **Note** This counter is only applicable to ETSI PRI.
ISDN_SUSPEND_RX	The number of ISDN Suspend messages received by the reporting call agent. **Note** This counter is only applicable to ETSI PRI.
ISDN_SUSPEND_ACK_TX	The number of ISDN Suspend Acknowledge messages sent from the reporting call agent. **Note** This counter is only applicable to ETSI PRI.
ISDN_SUSPEND_ACK_RX	The number of ISDN Suspend Acknowledge messages received by the reporting call agent. **Note** This counter is only applicable to ETSI PRI.
ISDN_SUSPEND_REJ_TX	The number of ISDN Suspend Reject messages sent from the reporting call agent. **Note** This counter is only applicable to ETSI PRI.
ISDN_SUSPEND_REJ_RX	The number of ISDN Suspend Reject messages received by the reporting call agent. **Note** This counter is only applicable to ETSI PRI.
ISDN_RESUME_TX	The number of ISDN Resume messages sent from the reporting call agent. **Note** This counter is only applicable to ETSI PRI.
ISDN_RESUME_RX	The number of ISDN Resume messages received by the reporting call agent. **Note** This counter is only applicable to ETSI PRI.
ISDN_RESUME_ACK_TX	The number of ISDN Resume Acknowledge messages sent from the reporting call agent. **Note** This counter is only applicable to ETSI PRI.

Table 15-9 ISDN Protocol Counters (continued)

Counter Label	Counter Context
ISDN_RESUME_ACK_RX	The number of ISDN Resume Acknowledge messages received by the reporting call agent. **Note** This counter is only applicable to ETSI PRI.
ISDN_RESUME_REJ_TX	The number of ISDN Resume Reject messages sent from the reporting call agent. **Note** This counter is only applicable to ETSI PRI.
ISDN_RESUME_REJ_RX	The number of ISDN Resume Reject messages received by the reporting call agent. **Note** This counter is only applicable to ETSI PRI.
ISDN_USER_INFO_TX	The number of ISDN User Information messages sent from the reporting call agent. **Note** This counter is only applicable to ETSI PRI.
ISDN_USER_INFO_RX	The number of ISDN User Information messages received by the reporting call agent. **Note** This counter is only applicable to ETSI PRI.
ISDN_CONG_CNTL_TX	The number of ISDN Congestion Control messages sent from the reporting call agent. **Note** This counter is only applicable to ETSI PRI.
ISDN_CONG_CNTL_RX	The number of ISDN Congestion Control messages received by the reporting call agent. **Note** This counter is only applicable to ETSI PRI.
ISDN_SEGMENT_TX	The number of ISDN Segment messages sent from the reporting call agent. **Note** This counter is only applicable to ETSI PRI.
ISDN_SEGMENT_RX	The number of ISDN Segment messages received by the reporting call agent. **Note** This counter is only applicable to ETSI PRI.

Call Processing Counters

Table 15-10 identifies the Call Processing counters and their meanings.

Table 15-10 Call Processing Counters

Counter Label	Counter Context
CALLP_ORIG_ATTMP	The number of originating call attempts of all types on the reporting call agent.
CALLP_TERM_ATTMP	The number of terminating call attempts of all types on the reporting call agent.
CALLP_ORIG_FAIL	The number of originating call attempts of all types that failed on the reporting call agent.
CALLP_TERM_FAIL	The number of terminating call attempts of all types that failed on the reporting call agent.
CALLP_CALL_SUCC	The number of successful originating and terminating call attempts of all types on the reporting call agent.
CALLP_CALL_ABAND	The number of originating call attempts of all types that were abandoned on the reporting call agent.

Table 15-10 Call Processing Counters (continued)

Counter Label	Counter Context
CALLP_ISDN_ORIG_ATTMP	The number of originating ISDN call attempts on the reporting call agent.
CALLP_ISDN_TERM_ATTMP	The number of ISDN terminating call attempts on the reporting call agent.
CALLP_ISDN_ORIG_FAIL	The number of ISDN originating call attempts that failed on the reporting call agent.
CALLP_ISDN_TERM_FAIL	The number of ISDN terminating call attempts that failed on the reporting call agent.
CALLP_ISDN_CALL_SUCC	The number of successful ISDN originating and terminating call attempts on the reporting call agent.
CALLP_ISDN_CALL_ABAND	The number of ISDN originating call attempts that were abandoned on the reporting call agent.
CALLP_SS7_ORIG_ATTMP	The number of originating SS7 call attempts on the reporting call agent.
CALLP_SS7_TERM_ATTMP	The number of SS7 terminating call attempts on the reporting call agent.
CALLP_SS7_ORIG_FAIL	The number of SS7 originating call attempts that failed on the reporting call agent.
CALLP_SS7_TERM_FAIL	The number of SS7 terminating call attempts that failed on the reporting call agent.
CALLP_SS7_CALL_SUCC	The number of successful SS7 originating and terminating call attempts on the reporting call agent.
CALLP_SS7_CALL_ABAND	The number of SS7 originating call attempts that were abandoned on the reporting call agent.
CALLP_SIP_ORIG_ATTMP	The number of originating SIP call attempts on the reporting call agent.
CALLP_SIP_TERM_ATTMP	The number of SIP terminating call attempts on the reporting call agent.
CALLP_SIP_ORIG_FAIL	The number of SIP originating call attempts that failed on the reporting call agent.
CALLP_SIP_TERM_FAIL	The number of SIP terminating call attempts that failed on the reporting call agent.
CALLP_SIP_CALL_SUCC	The number of successful SIP originating and terminating call attempts on the reporting call agent.
CALLP_SIP_CALL_ABAND	The number of SIP originating call attempts that were abandoned on the reporting call agent.
CALLP_MGCP_ORIG_ATTMP	The number of originating MGCP call attempts on the reporting call agent.
CALLP_MGCP_TERM_ATTMP	The number of MGCP terminating call attempts on the reporting call agent.
CALLP_MGCP_ORIG_FAIL	The number of MGCP originating call attempts that failed on the reporting call agent.
CALLP_MGCP_TERM_FAIL	The number of MGCP terminating call attempts that failed on the reporting call agent.
CALLP_MGCP_CALL_SUCC	The number of successful MGCP originating and terminating call attempts on the reporting call agent.

Table 15-10 Call Processing Counters (continued)

Counter Label	Counter Context
CALLP_MGCP_CALL_ABAND	The number of MGCP originating call attempts that were abandoned on the reporting call agent.
CALLP_CAS_ORIG_ATTMP	The number of originating CAS call attempts on the reporting call agent.
CALLP_CAS_TERM_ATTMP	The number of CAS terminating call attempts on the reporting call agent.
CALLP_CAS_ORIG_FAIL	The number of CAS originating call attempts that failed on the reporting call agent.
CALLP_CAS_TERM_FAIL	The number of CAS terminating call attempts that failed on the reporting call agent.
CALLP_CAS_CALL_SUCC	The number of successful CAS originating and terminating call attempts on the reporting call agent.
CALLP_CAS_CALL_ABAND	The number of CAS originating call attempts that were abandoned on the reporting call agent.
CALLP_ISDN_SS7_CALL	The number of successfully completed calls from an ISDN originator to an SS7 terminator on the reporting call agent.
CALLP_ISDN_ISDN_CALL	The number of successfully completed calls from an ISDN originator to an ISDN terminator on the reporting call agent.
CALLP_ISDN_SIP_CALL	The number of successfully completed calls from an ISDN originator to an SIP terminator on the reporting call agent.
CALLP_ISDN_MGCP_CALL	The number of successfully completed calls from an ISDN originator to an MGCP terminator on the reporting call agent.
CALLP_ISDN_CAS_CALL	The number of successfully completed calls from an ISDN originator to an CAS terminator on the reporting call agent.
CALLP_SS7_SS7_CALL	The number of successfully completed calls from an SS7 originator to an SS7 terminator on the reporting call agent.
CALLP_SS7_ISDN_CALL	The number of successfully completed calls from an SS7 originator to an ISDN terminator on the reporting call agent.
CALLP_SS7_SIP_CALL	The number of successfully completed calls from an SS7 originator to an SIP terminator on the reporting call agent.
CALLP_SS7_MGCP_CALL	The number of successfully completed calls from an SS7 originator to an MGCP terminator on the reporting call agent.
CALLP_SS7_CAS_CALL	The number of successfully completed calls from an SS7 originator to an CAS terminator on the reporting call agent.
CALLP_SIP_SS7_CALL	The number of successfully completed calls from a SIP originator to an SS7 terminator on the reporting call agent.
CALLP_SIP_ISDN_CALL	The number of successfully completed calls from a SIP originator to an ISDN terminator on the reporting call agent.
CALLP_SIP_SIP_CALL	The number of successfully completed calls from a SIP originator to an SIP terminator on the reporting call agent.
CALLP_SIP_MGCP_CALL	The number of successfully completed calls from a SIP originator to an MGCP terminator on the reporting call agent.
CALLP_SIP_CAS_CALL	The number of successfully completed calls from a SIP originator to an CAS terminator on the reporting call agent.

Table 15-10 Call Processing Counters (continued)

Counter Label	Counter Context
CALLP_MGCP_SS7_CALL	The number of successfully completed calls from an MGCP originator to an SS7 terminator on the reporting call agent.
CALLP_MGCP_ISDN_CALL	The number of successfully completed calls from an MGCP originator to an ISDN terminator on the reporting call agent.
CALLP_MGCP_SIP_CALL	The number of successfully completed calls from an MGCP originator to an SIP terminator on the reporting call agent.
CALLP_MGCP_MGCP_CALL	The number of successfully completed calls from an MGCP originator to an MGCP terminator on the reporting call agent.
CALLP_MGCP_CAS_CALL	The number of successfully completed calls from an MGCP originator to an CAS terminator on the reporting call agent.
CALLP_CAS_SS7_CALL	The number of successfully completed calls from an CAS originator to an SS7 terminator on the reporting call agent.
CALLP_CAS_ISDN_CALL	The number of successfully completed calls from an CAS originator to an ISDN terminator on the reporting call agent.
CALLP_CAS_SIP_CALL	The number of successfully completed calls from an CAS originator to an SIP terminator on the reporting call agent.
CALLP_CAS_MGCP_CALL	The number of successfully completed calls from an CAS originator to an MGCP terminator on the reporting call agent.
CALLP_CAS_CAS_CALL	The number of successfully completed calls from an CAS originator to an CAS terminator on the reporting call agent.
CALLP_INTERLA_ATTMP	The number of Interlata call attempts on the reporting call agent.
CALLP_INTERLA_FAIL	The number of Interlata call attempts that failed on the reporting call agent.
CALLP_INTERLA_SUCC	The number of Interlata call attempts that completed successfully on the reporting call agent.
CALLP_INTERLA_ABAND	The number of Interlata call origination attempts that were abandoned on the reporting call agent.
CALLP_INTRALA_ATTMP	The number of Intralata call attempts on the reporting call agent.
CALLP_INTRALA_FAIL	The number of Intralata call attempts that failed on the reporting call agent.
CALLP_INTRALA_SUCC	The number of Intralata call attempts that completed successfully on the reporting call agent.
CALLP_INTRALA_ABAND	The number of Intralata call origination attempts that were abandoned on the reporting call agent.
CALLP_INTL_ATTMP	The number of International call attempts on the reporting call agent.
CALLP_INTL_FAIL	The number of International call attempts that failed on the reporting call agent.
CALLP_INTL_SUCC	The number of International call attempts that completed successfully on the reporting call agent.
CALLP_INTL_ABAND	The number of International call origination attempts that were abandoned on the reporting call agent.

Table 15-10 Call Processing Counters (continued)

Counter Label	Counter Context
CALLP_EMGNCY_ATTMP	The number of Emergency call attempts on the reporting call agent.
CALLP_EMGNCY_FAIL	The number of Emergency call attempts that failed on the reporting call agent.
CALLP_EMGNCY_CALL_SUCC	The number of Emergency call attempts that completed successfully on the reporting call agent.
CALLP_EMGNCY_CALL_ABAND	The number of Emergency call origination attempts that were abandoned on the reporting call agent.
CALLP_LOCAL_ATTMP	The number of Local call attempts on the reporting call agent.
CALLP_LOCAL_FAIL	The number of Local call attempts that failed on the reporting call agent.
CALLP_LOCAL_SUCC	The number of Local call attempts that completed successfully on the reporting call agent.
CALLP_LOCAL_ABAND	The number of Local call origination attempts that were abandoned on the reporting call agent.
CALLP_TOLL_FREE_ATTMP	The number of Toll Free call attempts on the reporting call agent.
CALLP_TOLL_FREE_FAIL	The number of Toll Free call attempts that failed on the reporting call agent.
CALLP_TOLL_FREE_SUCC	The number of Toll Free call attempts that completed successfully on the reporting call agent.
CALLP_TOLL_FREE_ABAND	The number of Toll Free call origination attempts that were abandoned on the reporting call agent.
CALLP_H323_ORIG_ATTMP	The number of originating H323 call attempts on the reporting call agent.
CALLP_H323_TERM_ATTMP	The number of terminating H323 call attempts on the reporting call agent.
CALLP_H323_ORIG_FAIL	The number of originating H323 call attempts that failed on the reporting call agent.
CALLP_H323_TERM_FAIL	The number of terminating H323 call attempts that failed on the reporting call agent.
CALLP_H323_CALL_SUCC	The number of originating and terminating H323 call attempts that completed successfully on the reporting call agent.
CALLP_H323_CALL_ABAND	The number of terminating and originating H323 call attempts that were abandoned on the reporting call agent.
CALLP_ISDN_H323_CALL	The total number of successfully completed calls from an ISDN originator to an H323 terminator on the reporting call agent.
CALLP_SS7_H323_CALL	The total number of successfully completed calls from an SS7 originator to an H323 terminator on the reporting call agent.
CALLP_SIP_H323_CALL	The total number of successfully completed calls from a SIP originator to an H323 terminator on the reporting call agent.
CALLP_MGCP_H323_CALL	The total number of successfully completed calls from an MGCP originator to an H323 terminator on the reporting call agent.
CALLP_CAS_H323_CALL	The total number of successfully completed calls from a CAS originator to an H323 terminator on the reporting call agent.

Table 15-10 Call Processing Counters (continued)

Counter Label	Counter Context
CALLP_H323_SIP_CALL	The total number of successfully completed calls from an H323 originator to a SIP terminator on the reporting call agent.
CALLP_H323_ISDN_CALL	The total number of successfully completed calls from an H323 originator to an ISDN terminator on the reporting call agent.
CALLP_H323_SS7_CALL	The total number of successfully completed calls from an H323 originator to an SS7 terminator on the reporting call agent.
CALLP_H323_MGCP_CALL	The total number of successfully completed calls from an H323 originator to an MGCP terminator on the reporting call agent.
CALLP_H323_CAS_CALL	The total number of successfully completed calls from an H323 originator to a CAS terminator on the reporting call agent.
CALLP_H323_H323_CALL	The total number of successfully completed calls from an H323 originator to an H323 terminator on the reporting call agent.
CALLP_NAS_AUTH_SUCC	The total number of successful NAS Authentication Requests on the reporting call agent.
CALLP_NAS_AUTH_FAIL	The total number of failed NAS Authentication Requests on the reporting call agent.
CALLP_NAS_OP_FAIL	The total number of operation failures that occurred on the reporting call agent – typically indicative of a modem failure.
CALLP_NAS_ISP_PORT_LIMIT	The total number of NAS calls that failed on the reporting call agent due to the port limit of a modem being exceeded.
CALLP_NAS_NO_MODEMS	The total number of NAS calls that failed on the reporting call agent due to the unavailability of a modem.
CALLP_NAS_CLG_UNACC	The total number of NAS calls that failed on the reporting call agent due to the calling party number being blocked.
CALLP_NAS_CLD_UNACC	The total number of NAS calls that failed on the reporting call agent due to the called party number being blocked.
CALLP_NAS_USER_REQUEST	The total number of User Requests – Reason Code 801 – that are received in the DLCX messages on the reporting call agent.
CALLP_NAS_LOST_CARRIER	The total number of Lost Carrier – Reason Code 802 – that are received in the DLCX messages on the reporting call agent.
CALLP_NAS_LOST_SERVICE	The total number of Lost Service – Reason Code 803 – that are received in the DLCX messages on the reporting call agent.
CALLP_NAS_IDLE_TIMEOUT	The total number of Idle Timeout – Reason Code 804 – that are received in the DLCX messages on the reporting call agent.
CALLP_NAS_SESSION_TIMEOUT	The total number of Session Timeout – Reason Code 805 – that are received in the DLCX messages on the reporting call agent.
CALLP_NAS_ADMIN_RESET	The total number of Admin Reset – Reason Code 806 – that are received in the DLCX messages on the reporting call agent.
CALLP_NAS_ADMIN_REBOOT	The total number of Admin Reboot – Reason Code 807 – that are received in the DLCX messages on the reporting call agent.
CALLP_NAS_PORT_ERROR	The total number of Port Error– Reason Code 808 – that are received in the DLCX messages on the reporting call agent.

Table 15-10 Call Processing Counters (continued)

Counter Label	Counter Context
CALLP_NAS_NAS_ERROR	The total number of NAS Error– Reason Code 809 – that are received in the DLCX messages on the reporting call agent.
CALLP_NAS_NAS_REQUEST	The total number of NAS Request – Reason Code 810 – that are received in the DLCX messages on the reporting call agent.
CALLP_NAS_NAS_REBOOT	The total number of NAS Reboot– Reason Code 811 – that are received in the DLCX messages on the reporting call agent.
CALLP_NAS_PORT_UNNEEDED	The total number of Port Unneeded – Reason Code 812 – that are received in the DLCX messages on the reporting call agent.
CALLP_NAS_PORT_PREEMPTED	The total number of Port Pre-empted – Reason Code 813 – that are received in the DLCX messages on the reporting call agent.
CALLP_NAS_PORT_SUSPENDED	The total number of Port Suspended – Reason Code 814 – that are received in the DLCX messages on the reporting call agent.
CALLP_NAS_SERVICE_UNAVAIL	The total number of Service Unavailable – Reason Code 815 – that are received in the DLCX messages on the reporting call agent.
CALLP_NAS_CALLBACK	The total number of NAS Callback – Reason Code 816 – that are received in the DLCX messages on the reporting call agent.
CALLP_NAS_USER_ERROR	The total number of User Error – Reason Code 817 – that are received in the DLCX messages on the reporting call agent.
CALLP_NAS_HOST_REQUEST	The total number of Host Request – Reason Code 818 – that are received in the DLCX messages on the reporting call agent.
CALLP_IVR_NETWORK_REQ	The total number of requests for network based IVR service on the reporting call agent.
CALLP_IVR_NATIVE_REQ	The total number of requests for native IVR service on the reporting call agent.
CALLP_IVR_RESOURCE_FAIL	The total number of IVR sessions that could not be established on the reporting call agent.
CALLP_TOTAL_TDISC_ORIG_ATTMP	The total number of origination attempts by subscribers that are marked as temporarily disconnected, detected by the reporting call agent.
CALLP_ NLB_TEST_SUCC	The total number of successful Network Loop Back Tests completed by the reporting call agent.
CALLP_ NLB_TEST_FAIL	The total number of unsuccessful Network Loop Back Tests completed by the reporting call agent. This counter includes both call setup failures and resource failures. These are test calls abnormally released by the call agent due to reasons such as resource priorities.
CALLP_NCT_TEST_SUCC	The total number of successful Network Continuity Tests completed by the reporting call agent.
CALLP_ NCT_TEST_FAIL	The total number of unsuccessful Network Continuity Tests completed by the reporting call agent. This counter includes both call setup failures and resource failures. These are test calls abnormally released by the call agent due to reasons such as resource priorities.
CALLP_LB_TEST_SUCC	The total number of successful TDM Loop Back 108 Tests completed by the reporting call agent.

Table 15-10 Call Processing Counters (continued)

Counter Label	Counter Context
CALLP_TEST_ROUTE_SUCC	The total number of successful TDM Loop Back 108 Tests with DN dialed out in outgoing message completed by the reporting call agent.
CALLP_T38_FAX_MEDIA_SETUP_SUCC	This counter is incremented when the T.38 media connection is established successfully between the endpoints for T.38 fax transmission.
CALLP_T38_FAX_MEDIA_SETUP_FAIL	This counter is incremented when a T.38 media connection is not established successfully between the endpoints for T.38 fax transmission.

MGCP Adapter Counters

Table 15-11 identifies the MGCP Adapter counters provided in Release 4.5.

Table 15-11 MGCP Adapter Counters

Counter Label	Counter Context
MGCP_DECODE_ERROR	The number of MGCP messages received that failed decoding on the reporting call agent.
MGCP_ENCODE_ERROR	The number of MGCP messages to be sent that failed encoding on the reporting call agent.
MGCP_UNREACHABLE	The number of MGCP messages sent from the reporting call agent that failed due to the target gateway being unreachable.
MGCP_SEND_FAILED	The number of MGCP messages sent from the reporting call agent that failed while being sent to the target gateway.
MGCP_CRCX_ACK_RX	The number of MGCP CRCX acknowledgement messages received by the reporting call agent.
MGCP_CRCX_NACK_RX	The number of MGCP CRCX non-acknowledgement messages received by the reporting call agent.
MGCP_CRCX_TX	The number of MGCP CRCX messages sent by the reporting call agent.
MGCP_MDCX_ACK_RX	The number of MGCP MDCX acknowledgement messages received by the reporting call agent.
MGCP_MDCX_NACK_RX	The number of MGCP MDCX non-acknowledgement messages received by the reporting call agent.
MGCP_MDCX_TX	The number of MGCP MDCX messages sent by the reporting call agent.
MGCP_DLCX_RX	The number of MGCP DLCX messages received from gateways by the reporting call agent.
MGCP_DLCX_TX	The number of MGCP DLCX messages s.ent by the reporting call agent
MGCP_DLCX_ACK_RX	The number of MGCP DLCX acknowledgement messages received by the reporting call agent.
MGCP_DLCX_NACK_RX	The number of MGCP DLCX non-acknowledgement messages received by the reporting call agent.
MGCP_RQNT_ACK_RX	The number of MGCP RQNT acknowledgement messages received by the reporting call agent.
MGCP_RQNT_NACK_RX	The number of MGCP RQNT non-acknowledgement messages received by the reporting call agent.
MGCP_RQNT_TX	The number of MGCP RQNT messages sent by the reporting call agent.

Table 15-11 MGCP Adapter Counters

Counter Label	Counter Context
MGCP_AUEP_ACK_RX	The number of MGCP AUEP acknowledgement messages received by the reporting call agent.
MGCP_AUEP_NACK_RX	The number of MGCP AUEP non-acknowledgement messages received by the reporting call agent.
MGCP_AUEP_TX	The number of MGCP AUEP messages sent by the reporting call agent.
MGCP_NTFY_RX	The number of MGCP NTFY messages received from gateways by the reporting call agent.
MGCP_RSIP_RX	The number of MGCP RSIP messages received from gateways by the reporting call agent.
MGCP_RSIP_ACK_TX	The number of MGCP RSIP acknowledgement messages sent by the reporting call agent.
MGCP_AUCX_TX	The number of AUCX (Audit Connection) messages that were sent by the reporting call agent. (FUTURE – R5.0).
MGCP_AUCX_ACK_RX	The number of AUCX ACK (Audit Connection Acknowledgement) messages that were received by the reporting call agent. (FUTURE – R5.0).
MGCP_AUCX_NACK_RX	The number of AUCX NACK (Audit Connection NotAcknowlegement) messages that were received by the reporting call agent. (FUTURE – R5.0).

Session Initiation Protocol Counters

Table 15-12 identifies the Session Initiation Protocol counters provided in Release 4.5. These counters are common to several reporting types including SIM, AIN-SVC, POTS-MISC, and SIA.

Table 15-12 Session Initiation Protocol Counters

Counter Label	Counter Context
SIS_TOTAL_INCOM_MSG	The number of SIP messages the reporting call agent or feature server attempted to receive.
SIS_TOTAL_SUCC_INCOM_MSG	The number of SIP messages the reporting call agent or feature server successfully received.
SIS_TOTAL_OUTG_MSG_ATTMP	The number of SIP messages the reporting call agent or feature server attempted to send.
SIS_TOTAL_SUCC_OUTG_MSG	The number of SIP messages the reporting call agent or feature server successfully sent.
SIS_REQ_RETRAN_RX	The number of SIP request retransmission messages the reporting call agent or feature server received.
SIS_REQ_RETRAN_TX	The number of SIP request retransmission messages the reporting call agent or feature server sent.
SIS_RSP_RETRAN_RX	The number of SIP response retransmission messages the reporting call agent or feature server received.
SIS_RSP_RETRAN_TX	The number of SIP response retransmission messages the reporting call agent or feature server sent.
SIS_T1_TIMER_EXPIRED	The number of SIP T1 Timer expirations that occurred on the reporting call agent or feature server received over the collection interval.

Table 15-12 Session Initiation Protocol Counters (continued)

Counter Label	Counter Context
SIS_T2_TIMER_REACHED	The number of SIP T2 Timer expirations that occurred on the reporting call agent or feature server received over the collection interval.
SIS_INVITE_RX	The number of SIP INVITE messages the reporting call agent or feature server received.
SIS_INVITE_TX	The number of SIP INVITE messages the reporting call agent or feature server sent.
SIS_CANCEL_RX	The number of SIP CANCEL messages the reporting call agent or feature server received.
SIS_CANCEL_TX	The number of SIP CANCEL messages the reporting call agent or feature server sent.
SIS_BYE_RX	The number of SIP BYE messages the reporting call agent or feature server received.
SIS_BYE_TX	The number of SIP BYE messages the reporting call agent or feature server sent.
SIS_ACK_RX	The number of SIP ACK messages the reporting call agent or feature server received.
SIS_ACK_TX	The number of SIP ACK messages the reporting call agent or feature server sent.
SIS_OPTIONS_RX	The number of SIP OPTIONS messages the reporting call agent or feature server received.
SIS_OPTIONS_TX	The number of SIP OPTIONS messages the reporting call agent or feature server sent.
SIS_REGISTER_RX	The number of SIP REGISTER messages the reporting call agent or feature server received.
SIS_REGISTER_TX	The number of SIP REGISTER messages the reporting call agent or feature server sent.
SIS_INFO_RX	The number of SIP INFO messages the reporting call agent or feature server received.
SIS_INFO_TX	The number of SIP INFO messages the reporting call agent or feature server sent.
SIS_NOTIFY_RX	The number of SIP NOTIFY messages the reporting call agent or feature server received.
SIS_NOTIFY_TX	The number of SIP NOTIFY messages the reporting call agent or feature server sent.
SIS_100_RX	The number of 100 class (TRYING) messages the reporting call agent or feature server received.
SIS_100_TX	The number of 100 class (TRYING) messages the reporting call agent or feature server sent.
SIS_18x_RX	The number of 18x class (INFORMATIONAL) messages the reporting call agent or feature server received.
SIS_18x_TX	The number of 18x class (INFORMATIONAL) messages the reporting call agent or feature server sent.
SIS_200_RX	The number of 200 class (SUCCESS) messages the reporting call agent or feature server received.
SIS_200_TX	The number of 200 class (SUCCESS) messages the reporting call agent or feature server sent.
SIS_3xx_RX	The number of 3xx class (REDIRECTION) messages the reporting call agent or feature server received.
SIS_3xx_TX	The number of 3xx class (REDIRECTION) messages the reporting call agent or feature server sent.

Table 15-12 Session Initiation Protocol Counters (continued)

Counter Label	Counter Context
SIS_4xx_RX	The number of 4xx class (REQUEST FAILURES) messages the reporting call agent or feature server received.
SIS_4xx_TX	The number of 4xx class (REQUEST FAILURES) messages the reporting call agent or feature server sent.
SIS_5xx_RX	The number of 5xx class (SERVER FAILURES) messages the reporting call agent or feature server received.
SIS_5xx_TX	The number of 5xx class (SERVER FAILURES) messages the reporting call agent or feature server sent.
SIS_6xx_RX	The number of 6xx class (GLOBAL FAILURES) messages the reporting call agent or feature server received.
SIS_6xx_TX	The number of 6xx class (GLOBAL FAILURES) messages the reporting call agent or feature server sent.
SIS_7xx_RX	The number of 7xx class (RESERVED) messages the reporting call agent or feature server received.
SIS_7xx_TX	The number of 7xx class (RESERVED) messages the reporting call agent or feature server sent.
SIS_PROV_RSP_RETRAN_RX	The number of SIP provisioning response retransmission messages the reporting call agent or feature server received.
SIS_PROV_RSP_RETRAN_TX	The number of SIP provisioning response retransmission messages the reporting call agent or feature server sent.
SIS_PRACK_RX	The number of SIP PRACK messages the reporting call agent or feature server received.
SIS_PRACK_TX	The number of SIP PRACK messages the reporting call agent or feature server sent.
SIS_SUBSCRIBE_RX	The number of SIP SUBSCRIBE messages the reporting call agent or feature server received.
SIS_SUBSCRIBE_TX	The number of SIP SUBSCRIBE messages the reporting call agent or feature server sent.
SIS_REFER_RX	The number of SIP REFER messages the reporting call agent or feature server received.
SIS_REFER_TX	The number of SIP REFER messages the reporting call agent or feature server sent.
SIS_REFER_W_REPLACES_RX	The number of SIP REFER with REPLACES messages the reporting call agent or feature server received.
SIS_INVITE_REPLACES_TX	The number of SIP INVITE REPLACES messages the reporting call agent or feature server sent.
SIS_INVITE_REPLACES_RX	The number of SIP INVITE REPLACES messages the reporting call agent or feature server received.
SIS_REL100_RX	The number of REL100 class (TRYING) messages the reporting call agent or feature server received.
SIS_REL100_TX	The number of REL100 class (TRYING) messages the reporting call agent or feature server sent.
SIS_UNSUPPORTED_RX	The number of unsupported SIP messages the reporting call agent or feature server received.

Table 15-12 Session Initiation Protocol Counters (continued)

Counter Label	Counter Context
SIS_UPDATE_RX	The number of SIP UPDATE messages the reporting call agent or feature server received.
SIS_UPDATE_TX	The number of SIP UPDATE messages the reporting call agent or feature server sent.

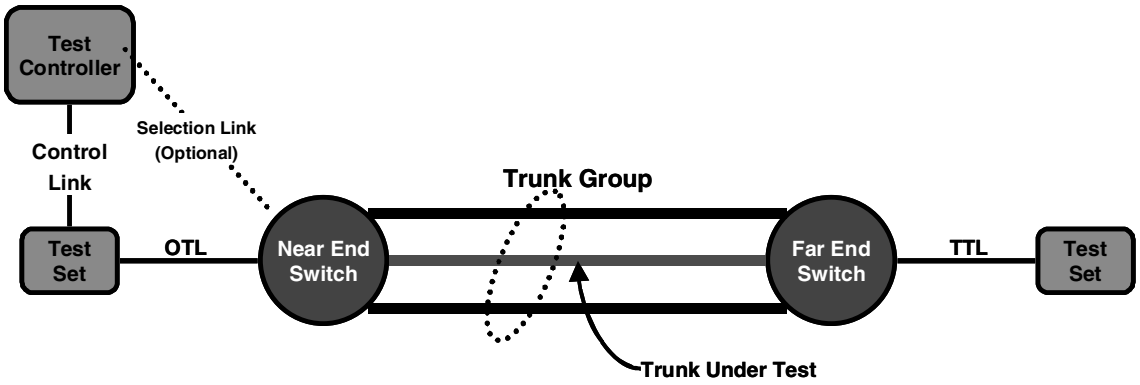
PSTN Trunk Testing

The legacy PSTN trunk network supports connection and performance appraisal testing individual trunks or network routes. This is generally referred to as 100-type tests. The Cisco BTS 10200 provides specific capabilities to support test call origination to selected individual trunks as well as test call termination.

Test Overview

Trunk testing is used to ascertain the transmission quality of the shared trunks used to interconnect switching systems. This is necessary because there is no other practical way to objectively determine each trunk's performance. Figure 15-1 depicts a typical trunk test system.

Figure 15-1 Typical Trunk Test System



The test controller is located on the originating side of the trunk test system. The controller selects a trunk group and a specific trunk within the trunk group to test. It then instructs the near end test equipment, which is connected to the OTL and switch to select the specified trunk and the destination number for the far end test set.

The near end switch then selects the Trunk Under Test (TUT) and, if the TUT is idle, dials the destination number through CAS or nonassociated signaling methods common to normal signaling for the trunk group. If the TUT is busy, an announcement is returned (usually reorder) towards the near end test set and the test call does not proceed.

The far end switch responds to the dialed digits by connecting to the far end test set via the TTL. The far end test set answers the call request. The near end and far end test equipment then conduct the required tests. The results are retrieved by the Test Controller.

The Cisco BTS 10200 supports OTL and TTL capability. User provided test equipment and, optionally, test controllers may be connected to the test lines. Interoperability between different carriers is ensured through proper selection of test equipment and test functions.

For the purposes of PSTN trunk testing, the near end is the Cisco BTS 10200 platform.

Cisco BTS 10200 Originating Test Line

This section discusses the following Cisco BTS 10200 originating test line information:

- Function, page 15-81
- Test Equipment, page 15-81
- Test Line, page 15-81
- Trunk Access, page 15-81
- Trunk Access and Test Termination Number Format, page 15-82
- Trunk Under Test Outpulsing, page 15-82

Function

The OTL originates all test calls. The OTL may be part of an automated trunk test system (for example, CAROT) that will select trunks, make test calls, conduct tests, record measurements and report marginal or inferior trunk performance.

Test Equipment

Test equipment capable of seizing the test line, outpulsing digits (preferably MF format), recognizing supervision, and supporting 1XX tests. While Cisco does not recommend any vendor, SAGE Instruments 930 or 935 series test equipment with the proper options are examples for use.

Test Line

Many gateway products can satisfy the OTL requirements. Preferred capabilities include

- Must be supported by the Cisco BTS 10200.
- T1 access line to connect to the test equipment to minimize transmission impairments caused by codecs and analog filters.
- Preferred signaling arrangement is wink start with MF signaling. (Other signaling arrangements can be supported).

Trunk Access

The Cisco BTS 10200 OTL can logically access up to 9,999 trunk groups, each with up to 9,999 trunks.

Conditions for trunk test access are met when either the requested trunk is in service and idle or the requested trunk is out of service or blocked. Trunk access is denied when the requested trunk is busy. If that happens, route advance is inhibited, and an announcement is returned.

Trunk Access and Test Termination Number Format

Figure 15-2 depicts the dialed digit format for accessing selected trunks and performing tests. These are the digits that the trunk test system or user actually dials. Figure 15-2 shows the format when the OTL is configured for MF signaling.

Figure 15-2 OTL Configured for MF Signaling

Test Type	Test Line	Dialed Digits 1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	Comment
Transmission Tests To Standard Test Lines	100	K P	Trunk Group Number				Member Trunk				1	0	0	S T						MW + QT
	101												1							Communications & Test
	102												2							MW
	103												3							Signal/Supervisory
	104												4							2-Way Tests
	105												5							CAROT ROTL/Responder
	N/A																			
	107												7							Data Transmission
	108												8							Digital Loopback
	109												9							Echo

Trunk Under Test Outpulsing

Once the specified trunk is selected, the Cisco BTS 10200 translates the dialed digits into a digit string for outpulsing. Once the trunk under test (TUT) is seized, it will outpulse the destination digits depicted in Figure 15-3. Since the digits may be sent by SS7, MF, or DTMF, only the actual destination digits are depicted.

Figure 15-3 Outpulsed Destination Digits

Test Type	Test Line	Dialed Digits 1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	Comment
Transmission Tests	100	9	5	8	1	1	0	0												100 Test Line Group
	101							1												101 Test Line Group
	102							2												102 Test Line Group
	103							3												103 Test Line Group
	104							4												104 Test Line Group
	105							5												105 Test Line Group
	N/A																			N/A
	107							7												107 Test Line Group
	108							8												108 Test Line Group
	109							9												109 Test Line Group

Cisco BTS 10200 Terminating Test Line

This section discusses the following Cisco BTS 10200 terminating test line information:

- Function, page 15-83
- Test Equipment, page 15-83
- Test Line, page 15-83
- TTL Dial Plan, page 15-83

Function

The TTL terminates all test calls. The TTL may be a responder capable of interacting with an automated trunk test system (for example, CAROT) or it may be a manual test line termination.

Test Equipment

Test equipment must be capable of recognizing an incoming call request from the test line, returning an answer signal, recognizing supervision, and supporting 1XX tests. Although Cisco does not recommend any vendor, SAGE Instruments 930 or 935 series test equipment with the proper options are good choices.

Test Line

Many gateway products can satisfy the OTL requirements. Preferred capabilities include

- Must be supported by the Cisco BTS 10200.
- T1 access line to connect to the test equipment to minimize transmission impairments caused by codecs and analog filters.
- Preferred signaling arrangement is immediate start with no incoming digits. (Other signaling arrangements can be supported).

TTL Dial Plan

The Cisco BTS 10200 test lines are typically assigned 958-11XX numbers as depicted in Figure 15-4. Any line or trunk may dial the appropriate digits to reach a TTL. Other dial plans are also supported and may also work in conjunction with the depicted plan.

Figure 15-4 958-11XX Number Assignment

Test Type	Test Line	Dialed Digits 1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	Comment
Transmission Tests	100	9	5	8	1	1	0	0												100 Test Line Group
	101							1												101 Test Line Group
	102							2												102 Test Line Group
	103							3												103 Test Line Group
	104							4												104 Test Line Group
	105							5												105 Test Line Group
	N/A																			N/A
	107							7												107 Test Line Group
	108							8												108 Test Line Group
	109							9												109 Test Line Group

Near End Test Origination Test Line

The BTS 10200 supports calls used to test individual trunks that connect a local gateway with a gateway or PSTN switch at a remote office. The BTS 10200 supports OTL and TTL capability. User-provided test equipment and, optionally, test controllers can be connected to the test lines. Proper selection of test equipment and test functions helps to ensure interoperability between different carriers.

The processes described in this section are applicable to the BTS 10200. The processes might work differently on other switches.

The process for testing a BTS 10200 OTL is as follows:

1. The user verifies that the remote CO has the desired 1xx test line available.
2. The user sets up a test device on a CAS TGW that is connected to the local BTS 10200.
3. The user provisions the CAS-TG-PROFILE table, setting TEST-LINE = YES. (Provisioning commands are described in the Cisco BTS 10200 Softswitch CLI Database.)
4. On the test device at the CAS TGW side, the user enters digits representing the circuit to be tested and the test to be performed:
   - TG, for example 0003
   - Trunk number, for example 0018

     The complete trunk address in this example is 00030018.
   - Test type (10x), for example 104

     The technician dials KP-00030018-104-ST.
5. The BTS 10200 automatically inserts either 9581 or 9591 in front of the test type digits to create a dialing string.

   The complete test string in this example is PREFIX | 00030018 | 9581104 | END.

Note Alternatively, with the BTS 10200, the user can dial the test type with the 9581 or 9591 included: KP-00030018-9581104-ST.

6. The BTS 10200 selects the trunk to be tested based on the user-defined trunk address.
7. The TGW outpulses the digits to the remote switch over the designated trunk.

Far End Originating Test Line

The far end originating test line (OTL) may be located on a different switch product as well as on a different carrier (for example, ILEC, IXC, CLEC). The far end OTL connects to the near end Cisco BTS 10200 softswitch TTL through the TUT. This section discusses the following Cisco BTS 10200 far end originating test line information:

- Function, page 15-85
- Test Equipment, page 15-85
- Test Line, page 15-85
- Trunk Access, page 15-85
- Trunk Access and Test Termination Number Format, page 15-85
- Trunk Under Test Outpulsing, page 15-85

Function

The OTL originates all test calls towards the Cisco BTS 10200 softswitch. The OTL may be part of an automated trunk test system (for example, CAROT) that will select trunks, make test calls, conduct tests, record measurements and report marginal or inferior trunk performance.

Test Equipment

Test equipment capable of seizing the test line, outpulsing digits, recognizing supervision, and supporting 1XX tests. Although Cisco does not recommend any vendor, SAGE Instruments 930 or 935 series test equipment with the proper options are good choices.

Test Line

OTL requirements are specific to the Far End switch product as well as to far end service provider/enterprise test methods and procedures. That subject, however, is outside the scope of this document.

Trunk Access

This is specific to the far end switch product and outside the scope of this document.

Trunk Access and Test Termination Number Format

This is specific to the far end switch product and outside the scope of this document.

Trunk Under Test Outpulsing

The far end switch translates the dialed digits into a digit string for outpulsing. The Cisco BTS 10200 softswitch expects to receive destination digits depicted in Figure 15-5. Since the digits might be sent through SS7, MF, or DTMF, only the actual destination digits are depicted.

Figure 15-5 Received Destination Digits

Test Type	Test Line	Dialed Digits 1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	Comment
Transmission Tests	100	9	5	8	1	1	0	0												100 Test Line Group
	101							1												101 Test Line Group
	102							2												102 Test Line Group
	103							3												103 Test Line Group
	104							4												104 Test Line Group
	105							5												105 Test Line Group
	N/A																			N/A
	107							7												107 Test Line Group
	108							8												108 Test Line Group
	109							9												109 Test Line Group

Far End Terminating Test Line

This section discusses the following Cisco BTS 10200 far end terminating test line information:

- Function, page 15-86
- Test Equipment, page 15-86
- Test Line, page 15-86
- TTL Dial Plan, page 15-86

Function

The TTL terminates all test calls. The TTL may be a responder capable of interacting with an automated trunk test system (for example, CAROT) or it may be a manual test line termination.

Test Equipment

Test equipment capable of recognizing an incoming call request from the test line, returning an answer signal, recognizing supervision, and supporting 1XX tests. Although Cisco does not recommend any vendor, SAGE Instruments 930 or 935 series test equipment with the proper options are good choices.

Test Line

OTL requirements are specific to the far end switch product as well as far end service provider/enterprise test methods and procedures. This is outside the scope of this document.

TTL Dial Plan

Test lines are typically assigned 958-11XX numbers as depicted in Figure 15-6.

Figure 15-6 958-11XX Number Assignments

Test Type	Test Line	Dialed Digits 1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	Comment
Transmission Tests	100	9	5	8	1	1	0	0												100 Test Line Group
	101							1												101 Test Line Group
	102							2												102 Test Line Group
	103							3												103 Test Line Group
	104							4												104 Test Line Group
	105							5												105 Test Line Group
	N/A																			N/A
	107							7												107 Test Line Group
	108							8												108 Test Line Group
	109							9												109 Test Line Group

1xx Test Lines

This section discusses the following Cisco BTS 10200 1xx test line information:

- 1xx Test Line Support, page 15-87
- 100 Test–Balance, page 15-88
- 101 Test–Communications and Test, page 15-88
- 102 Test–Milliwatt, page 15-88
- 103 Test–Signaling and Supervisory, page 15-88
- 104 Test–2-Way Test, page 15-88
- 105 Test–ROTL/Responder, page 15-88
- 107 Test Line–Data Transmission, page 15-89
- 108 Test–Digital Loopback, page 15-89
- 109 Test–Echo, page 15-89

1xx Test Line Support

When the BTS 10200 is the near-end switch, the following process takes place at the remote switch:

1. The remote switch recognizes the trunk test prefix (9581 or 9591) on the incoming signal, and it uses the test type to route the test to the appropriate test line.
2. The appropriate tests are performed on the test set.
3. Additional test processes may be used, depending on the specific test configuration.

When the BTS 10200 is supporting the TTL capability (test call originated at another switch), the BTS 10200 receives the 958 or 959 call, recognizes the 958 or 959 type, and routes the test to the appropriate test line.

The BTS 10200 enables a TDM-based testing device to perform continuity testing over an MF CAS TDM trunk interface. An MGCP-based trunking gateway must be present in the test path. The TDM test type is the traditional 1xx test type, with an additional enhancement—the ability to route the test call to a specified DN on a given trunk circuit.

100 Test–Balance

The balance test is normally used for two-wire switches to ascertain the performance of the four-wire terminating set "4WTS" or hybrid. Improper options or equipment faults can cause the trunk to sound hollow or have an echo.

This test can also be used to determine the far to near loss of the trunk under test, in some cases, as well as the far to near noise.

When called, the far end test set will either immediately answer with a quiet termination (silence) or provide a milliwatt test tone for a brief period.

101 Test–Communications and Test

This test supports testers to evaluate the TUT by actually talking over it. Normally, the test line is routed to a test position. It also supports manual or specialized testing across the TUT.

102 Test–Milliwatt

The milliwatt test provides a test tone throughout the test. Periodically, the tone may be removed automatically by the far end test set for a brief period of approximately 1 second in every 10 seconds. This helps failed T1 lines to regain frame synchronization and may also be used for other purposes.

This test may be used to determine the far to near loss and/or C-Notched noise of the trunk under test. It may also be used for other far to near test purposes.

103 Test–Signaling and Supervisory

The 103 test provides a connection to a supervisory and signaling test circuit for overall testing of these features on intertoll trunks equipped with ring forward.

104 Test–2-Way Test

Supports far to near and near to far evaluation for the TUT. The operation is very simple with the far end test equipment proceeding through a specific sequence of test steps.

The 104 test supports 2-way transmission testing and 2-way noise checking.

105 Test–ROTL/Responder

This is the preferred test line as it supports many tests for either the near to far or far to near direction. The near end test equipment is normally able to communicate with the far end test equipment to set up and conduct specified tests.

For example, the SAGE 930/935 test sets provide a robust menu of tests that include phase hits, jitter, and nonlinear distortion.

The 105 test line is normally used by CAROT and other automated trunk test systems as the far end test line. In CAROT terms, this is commonly called the responder.

107 Test Line–Data Transmission

The data transmission test line supports 1-way testing of certain voice band data parameters. This includes peak to average ratio signal (PAR), slope, quiet termination, and intermodulation distortion test signals.

It should be noted that newer test equipment, like the SAGE 930/935, provides these and other voice band data tests for *both* directions makes it possible to use one test line to evaluate voice and voice band data performance.

108 Test–Digital Loopback

The 108 test line supports testing by means of a digital loopback. The T108 test line feature determines the performance of trunks connecting digital exchange switches, including voice over packet (VoP) softswitches. BTS 10200 incoming trunks requesting other 1xx-type test lines are routed to shared test lines for the requested tests, regardless of which gateway terminates the trunk or which gateway/IAD terminates the test line. The T108 test line feature requests a test to be performed within the same gateway where the trunk under test (TUT) is terminated, and provides a digital loopback within the gateway. The T108 test line feature supports manual and automated testing.

The T108 test line sequence is as follows:

1. The near-end switch originates the test sequence by placing a test call, identifying the trunk to be selected, and the test line number. A digital test pattern generator is used in the test setup shown in Figure 15-1.
2. The near-end switch uses the trunk identifier to override normal call processing and select only the requested trunk.
3. The far-end switch responds to the destination number and connects to the T108 test line. The T108 test line enables a digital loopback.
4. When the near-end switch receives answer supervision, it conducts digital test sequences to ascertain trunk performance.
5. Once the test sequences are completed, the near-end switch releases the test call and both switches release the trunk connection.
6. The far-end switch can detect if the test connection exceeds a preset time and releases the test connection if the preset time is exceeded.

The T108 test line is also used for trunk redirection (wholesale dial) for Internet services where the carrier modem termination is integrated into the trunk gateway. In this case, the integral digital stored program (DSP) normally supports modem-only transmissions.

109 Test–Echo

The 109 test line supports in-service testing of echo cancellers or echo suppressors.

CHAPTER 16

Disaster Recovery Procedures

Revised: July 22, 2009, OL-8000-32

Introduction

This chapter describes how to recover your database in a disaster situation, how to recover your database from another database, and how to recover data from the Call Agent shared memory.

Cisco recommends backing up all data on the Element Management System (EMS), Call Agent (CA) and Feature Server (FS) platforms on a daily basis, and saving the backed up data to a remote server. Data backup files are needed in the unlikely event that data on both the primary and secondary sides of any platform become corrupted. In that case, data must be restored from a backup file.

Restarting a Cisco BTS 10200 Softswitch Process

When a Cisco BTS 10200 Softswitch process exits due to an internal error (such as SIGSEGV on UNIX) or is terminated by the platform, the system automatically restarts the process that shut down.

Restarting the process is a preferred alternative to switching over to the mate, because the restart preserves stable calls and also attempts to preserve transient calls. When a process is restarted, the process audits information such as resource states and attempts to repair inconsistencies. If a process experiences a high failure rate (even after repeated restarts), the system will switch over to the mate.

Disaster Recovery From Flash Archive

This section describes the steps needed to restore the Flash Archive on the Cisco BTS 10200 Softswitch system. The flash archive backup is performed before any software upgrade or for maintenance routine purpose. This procedure is used ONLY when both mirrored disks are corrupted or cannot be booted.

Flash Archive is a Sun Solaris tool that allows you to take an image of a host and store it on a network file server (NFS) that can be used later for disaster recovery.

For the Cisco BTS 10200 Softswitch, it is recommended to take a system flash archive whenever the Solaris Operation System is being modified.

Before You Begin

Before restoring your system, you must have the following:

- Bootable Sun Solaris 10 Operating System CD #1
  Note: Sun Solaris 10 can be download at www.sun.com
- Console access
- Restored Host name
- Internet Protocol (IP) address and netmask of restored system
- Location of an archive
- Enabling negotiation on the 2900 switch for the primary interface of the system

Example:

```
c2924.118-A#config t
c2924.118-A(config-t)#int fastEthernet 0/1
c2924.118-A(config-if)#no speed 100
c2924.118-A(config-if)#no full duplex
```

Flash Archive Restore

Note Cisco recommends running this procedure during maintenance window or when traffic is low.

Step 1 Connect to the console of the restored unit.

Step 2 Load the *bootable Solaris-10 CD* into the compact disk - read only media (CD-ROM) drive.

Step 3 At the *ok*> prompt, type: **boot cdrom**

Step 4 Enter **0** for English.

Step 5 Enter **14** for Other.

Step 6 Enter **vt100** for terminal type.

Step 7 Press **Esc-2** to continue.

Step 8 Press **Esc-2** again to continue.

Step 9 Press **Esc-2** to continue, use default setting (Mark **X** on *Yes* for Networked).

Step 10 Choose primary interface then **Esc-2** to continue.

Step 11 Press **Esc-2** to continue, use default setting (Mark **X** on *No* for Use Dynamic Host Configuration Protocol (DHCP)).

Step 12 Enter <hostname>, then press **Esc-2** to continue.

Step 13 Enter <IP address>; then press **Esc-2** to continue.

Step 14 Press **Esc-2** to continue, use default setting (Mark **X** on *Yes* for System part of a subnet).

Step 15 Enter <Netmask>; then press **Esc-2** to continue.

Step 16 Press **Esc-2** to continue, use default setting (Mark **X** on *No* for Enable IPv6).

Step 17 Confirm the network information and press **Esc-2** to continue.

Step 18 Press **Esc-2** to continue, use default setting (Mark **X** on *No* for Configure Kerberos Security).

Step 19 Press **Esc-2** to continue.

Step 20 Mark **X** on *None* for Name service. Press **Esc-2** to continue.

Step 21 **Confirm the information and press** Esc-2 **to continue.**

Step 22 Choose Continents and Oceans then **Esc-2.**

Step 23 Choose Countries and Regions then Press **Esc-2.**

Step 24 Mark X on Timezone. Press Esc-2 to continue.

Step 25 Set date and time. Press **Esc-2** to continue.

Step 26 Confirm the information and press **Esc-2** to continue.

Step 27 Choose **F4** for Flash installation, **Esc-4**.

Step 28 Choose **Manual reboot**, then Press **Esc-2**.

Step 29 Mark **x** on NFS for NFS Flash Archive Retrieval Method then Press **Esc-2**.

Step 30 Provide the location of the archive, as shown in the following example and Press **Esc-2**:

```
10.89.224.1:/archive/prica18.archive
```

Press **Esc-2** to continue.

Step 31 Mark **x** on primary Disk and then Press **Esc-2**.

Step 32 Press **Esc-2** to continue without preserve data.

Step 33 Press **Esc-4** for Customize disk layout.

Step 34 Partition the disk as follows and Press **Esc-2.**

```
filesys rootdisk.s0 2000 /
filesys rootdisk.s1 5000 /var
filesys rootdisk.s3 4000 swap
filesys rootdisk.s4 24
filesys rootdisk.s5 free /optfilesys rootdisk.s6 2000
```

Press **Esc-2** to confirm Disk Layout.

Step 35 Press **Esc-2** to continue.

Step 36 Press **Esc-2** to continue without remote mounts.

Step 37 Press **Esc-2** to continue with installation.

Note The restoration will take about 15-30 minutes.

Step 38 Press ! (exclanation sign) to exit if prompted.

Step 39 Verify /a/etc/vfstab and /a/etc/system files contain no disk mirroring information.

Example of /a/etc/vfstab:

```
#######################################################
#device device mount FS fsck mount mount
#to mount to fsck point type pass at boot options
#
#/dev/dsk/c1d0s2 /dev/rdsk/c1d0s2 /usr ufs 1 yes -
fd - /dev/fd fd - no -
/proc - /proc proc - no -
/dev/dsk/c1t0d0s3 - - swap - no -
/dev/dsk/c1t0d0s0 /dev/rdsk/c1t0d0s0 / ufs 1 yes -
```

```
/dev/dsk/c1t0d0s1 /dev/rdsk/c1t0d0s1 /var ufs 1 yes -
/dev/dsk/c1t0d0s5 /dev/rdsk/c1t0d0s5 /opt ufs 2 yes -
swap - /tmp tmpfs - yes -
########################################################
```

/a/etc/system file **SHOULD NOT** have the following similar lines:

```
##############################
* Begin MDD root info (do not edit)
rootdev:/pseudo/md@0:0,2,blk
* End MDD root info (do not edit)
##############################
```

Step 40 Enter the following command:

```
cp /a/bin/date /a/bin/.date
mv /a/bin/date.archive /a/bin/date
mv /a/etc/rc3.d/S99platform /a/etc/rc3.d/saved.S99platform
```

Step 41 Restore 2900 switch back to force 100MB full-duplex.

Step 42 Power cycle the system.

Setting up Interfaces

Use the following procedures to set-up the interfaces.

Step 1 Login as root.

Step 2 Sftp the following files from the mate:

```
cd /tmp
sftp <mate ip address>
get /etc/resolv.conf
get /etc/hosts host
get /etc/netmasks
get /etc/nsswitch.conf
get /etc/default/init
bye
```

Step 3 Copy the nsswitch.conf file to /etc/ directory

```
cp –p nsswitch.conf /etc/
```

Step 4 Copy the nsswitch.conf file to /etc/ directory

```
cp –p nsswitch.conf /etc/
```

Step 5 Copy the resolv.conf file to /etc/ directory

```
cp –p resolv.conf /etc/
```

Step 6 Copy init file to /etc/default/ directory

```
cp –p init /etc/default/
```

Step 7 Set up interfaces:

```
cd /opt/setup
setlogic_EMS.sh (Run this script to set up interfaces on EMS box)
setlogic_CA.sh ( Run this script to set up interfaces on CA box)

Verify all interfaces are setting up properly.
```

Step 8 Set up root password by enter the following command:

```
passwd root
```

Step 9 Reboot the box:

```
shutdown –y –g0 –i6
```

Restoring the Cisco BTS 10200 Softswitch Application

To restore the software application, perform the following steps:

Step 1 Login as root.

Step 2 Run **checkCFG** script to make sure no errors are encounter.

Step 3 Restore platforms shared-memory.

For CA/FS:

```
<hostname>#mount <NFS server ip>:/<shared directory> /mnt
<hostname>#cp /mnt/data.<hostname>.CA.gz /opt/
<hostname>#gzip -cd /opt/data.<hostname>.CA.gz | tar -xvf -
<hostname>#cp /mnt/data.<hostname>.FSPTC.gx /opt/
<hostname>#gzip -cd /opt/data.<hostname>.FSPTC.gz | tar -xvf -
<hostname>#cp /mnt/data.<hostname>.FSAIN.gz /opt/
<hostname>#gzip -cd /opt/data.<hostname>.FSAIN.gz | tar -xvf -
```

For EMS/BDMS:

```
<hostname>#mount <NFS server ip>:/<shared directory> /mnt
<hostname>#cp /mnt/oradata.<hostname>.gz /opt/
<hostname>#cp /mnt/db.<hostname>.gz /opt/
<hostname>#gzip -cd /opt/oradata.<hostname>.gz | tar -xvf -
```

Step 4 Reboot the system.

```
<hostname>#sync;sync;
<hostname>#shutdown -y -g0 -i6
```

Step 5 Bring up BTS application.

```
<hostname>#platform start
```

Step 6 Restore platform startup script.

```
<hostname>#mv /etc/rc3.d/saved.S99platform /etc/rc3.d/S99platform
```

Step 7 Refer to Jumpstart documentation to set up disk mirroring.

Note Cisco recommends running this procedure during maintenance window or when traffic is low.

Power Failure Recovery

One critical component of the Cisco BTS 10200 Softswitch software is the memory resident database, also referred to as ***Shared Memory***. Shared memory can be damaged by internal/external power supply failure.

The local status indicator for the shared memory database indicates that all actions needed to synchronize this database with the Active side while on standby have been completed. This status is tested when a platform starts up as Active. If the target state is Standby, the status indicator does not affect the normal startup sequence.

Power Fail Occurs Procedure

If power failure occurs, do the following:

1. Check the state of the surviving hosts and make sure that all platforms are still running.
2. Check the alarm logs if the EMS is available.

Power is Restored Procedure

When power comes back on, the Cisco BTS 10200 Softswitch software and all platforms should power up running in duplex Active/Standby.

Step 1 Use the **nodestat** command to verify that all platforms are running with no failure indication.

Step 2 If the platform shuts down or fails to come up, perform the following steps to determine the cause of the problem and determine the action to resolve it:

a. Check the alarm logs to verify the system status.

b. Trace logs display the most significant events about the state of the platforms.

c. Check and analyze the logs for details that may provide the cause of the failure.

Power Failure Scenarios

The following power failure scenarios are discussed in the following sections:

- Power Failure on Single Host Computer, page 16-7

  Only one host of the two mated host computers is affected by the power outage.
- Power Failure on Both Call Agent Computers, page 16-8

  Both mated host Call Agent computes are affected by the power outage.
- Power Failure on Both Element Management System Computers, page 16-9

  Both mated host EMS computers are affected by the power outage,
- Total System Power Outage, page 16-9

  All hosts computers are affected by the power outage.

Power Failure on Single Host Computer

If power failure occurs on one of the two sides while starting up a Standby platform, it can result in corrupted shared memory. The status indicator for the shared memory database will report 'shared memory database in bad state' if the Standby platform is restarted as the Active platform.

Recovery Procedure

Depending on the state of the Mate host computer, the following procedure are the alternatives on how to proceed:

No Failures on the Surviving Host

Step 1 Verify that all platforms are running as Active.

Step 2 If all platforms are running as Active, restore power. Restoring power restarts all platforms running as Standby on the failing host.

Platform Failure on the Surviving Host

Step 1 If power failure occurred while the surviving host computer is being brought up, restart the failing platform ***immediately*** (before power is restored on the other host).

Step 2 If the procedure does not work and reports a *'bad state'* for the shared memory, proceed to clear the shared data area and wait for the mate to be restarted.

Step 3 When power is restored, verify that all platforms are running by entering the **nodestat** command on the recovering host computer.

Step 4 Restart the failing platform on the host computer that is not affected by the power outage. The platform should come up as Standby.

Platform Failure Not Due To 'Bad State' of the Shared Memory on the Mate Host Computer or Any Failure on the Recovering Host Computer

Step 1 Check the alarm logs and search for alarms belonging to the failing platforms.

Step 2 The trace logs display the most significant events about the state of the platforms.

Step 3 Check and analyze the logs for details that may provide the cause of the failure. If possible, fix the problem.

a. If the system can run in simplex, send the logs to Cisco Technical Assistance Center (TAC) for diagnosis and assistance.

b. If the system cannot run simplex, run the procedure for a duplex power failure.

Power Failure on Both Call Agent Computers

Step 1 If any platforms start, take them down first.

Step 2 Clear data directories on both sides and perform a fresh download from the EMS, as shown in the following steps. Do the following on all platforms:

a. Enter the following command:

```
cd <platform>/bin/data; rm *
```

b. Restart both sides using the following command:

```
platform start all
```

c. Do a fresh download (extract Oracle data from the EMS and send it to the Call Agent). See the *Cisco BTS 10200 Softswitch Command Line Interface Guide* for the commands.

d. Check transaction queue - make sure data is going from the EMS to the CA.

e. Enter the command **audit db ems** to make sure everything is in sync.

Step 3 Discrepancies will have to be fixed via command line interface (CLI) commands.

Caution This may take hours to complete and during this time, call processing is lost, that is why it is critical that there is no common single point of failure in the power feeds.

Power Failure on Both Element Management System Computers

Step 1 If the platforms start, shut them down first.

Step 2 Audit the Oracle database.

Step 3 Check the mysql database.

Step 4 Restart both sides using the following command:

```
platform start all
```

Step 5 Enter the command **audit db ems** to make sure everything is in sync.

Step 6 Discrepancies will have to be fixed via CLI commands.

Caution This may take hours to complete and during this time, call processing is lost, that is why it is critical that there is no common single point of failure in the power feeds.

Total System Power Outage

Step 1 If the platforms start, take them down first.

Step 2 Audit the Oracle database.

Step 3 Check the mysql database.

Step 4 Clear the data directories on both CallAgent sides and do a fresh download from the EMS.

Step 5 On all platforms repeat the following steps:

a. Enter the following command:

```
cd <platform>/bin/data; rm *
```

b. Restart both sides using the following command:

```
platform start all
```

c. Do a fresh download (extract Oracle data from the EMS and send it to the Call Agent). See the *Cisco BTS 10200 Softswitch Command Line Interface Guide*.

d. Check the transaction queue to make sure that data is going from the EMS to the CA.

e. Enter the command **audit db ems** to either make sure everything is in sync.

Step 6 Discrepancies will have to be fixed via CLI commands.

Caution This may take hours to complete and during this time, call processing is lost, that is why it is critical that there is no common single point of failure in the power feeds.

Element Management System Database Recovery from Hot Backup

This section provides procedures to restore your Oracle EMS database data files from the most current hot backup and then recover your database from the backup. If additional archive log backup (by ora_arch_backup.ksh) was done after the hot backup, the additional archive log backup file sets need to be restored also. All of these backup file sets are assumed to be located on the remote FTP site.

Directory to restore backup files: */opt/oraback*.

The following assumptions were made for this procedure:

Daily backup schedule:

2:00 AM – daily hot backup (by ora_hot_backup.ksh process)

18:00 PM – daily archive log backup (by ora_arch_backup.ksh process)

Oracle databases on both primary and secondary EMS systems crashed completely at January 10, 2002, 20:00pm.

Recovery Goal

The goal in the scenario above is to recover the primary EMS Oracle database by using your most recent backups.

In this case, since the database crashed January 10, 2002, 20:00pm, the backup file sets with timestamp '200201100200' from 2:00am hot backup and those with timestamp '200201101800' from 18:00 archive log backup must be restored. Timestamp is formatted as YYYYMMDDhhmm.

If your database crashes before the archive log backup, you only need to restore the 2:00 am hot backup file sets.

If your system does not perform extra archive log backup daily by ora_arch_backup.ksh, use backup file sets from hot backup only.

In this sample scenario, the primary EMS database will be recovered first to resume operation. Then the secondary EMS will be recovered using the procedures that recover data from the primary EMS.

Note Before this recovery process is applied, it is assumed that the entire system, including all corrupted applications, has been restored.

Recovering the Primary Element Management System Database

Perform the following procedure on the primary EMS system to recover the primary EMS database from your most recent backup files:

Step 1 Make sure the platform is shut down and the system cron process has stopped.

Step 2 Log in as **root**.

Step 3 Enter the following commands to shut down the system:

```
platform stop all

svcadm disable svc:/system/cron
```

Note Execute *platform stop all* and *stop_cron.sh* on the secondary EMS also if the secondary EMS platform is active.

Step 4 Log in as **oracle** user, or **su – oracle.**

Step 5 Enter the following command to verify that there is enough free disk space:

```
df -k /opt/oraback
```

The EMS system must have enough disk space in the */opt/oraback* directory to restore all database data files and archive log files. The database data files can take up to 3.6 gigabits (GB) if it is fully populated with data; each archivelog file requires 5MB additional space. The number of archivelog files in the backup set can be identified from the optical1_ora_hot_full_backup_<timestamp>.log and/or the optical1_ora_arc_incr_backup_<timestamp>.log file in */opt/oraback* directory.

Step 6 Restore targeted backup file sets from the remote FTP site.

FTP the targeted database backup file sets from the remote FTP server to the */opt/oraback* directory on the EMS system. Then uncompress all the *.Z* files.

a. **Enter the following commands:**

```
cd /opt/oraback
ftp <remote_ftp_server>
```

b. Log in as **oracle**.

c. Enter the password (default password is *ora00*).

d. **Enter the following commands:**

```
ftp cd <remote_backup_directory>
ftp bin (* Use binary transfer mode *)
```

e. Get the following files. If archivelog backup is not performed, get only the hot backup files.

Backup files from 2:00 hot backup:

- optical1_arc_full_1_167:200201100200.Z
- optical1_arc_full_1_168:200201100200.Z
- optical1_ctl_binary: 200201100200.Z
- optical1_ctltrc:200201100200:tar.Z
- optical1_hot_full_1_166:200201100200.Z

- optical1_ora_hot_full_backup_200201100200.log

Back up files from the 18:00 archivelog backup:

- optical1_arc_incr_1_169:200201101800.Z
- optical1_ctl_binary:200201101800.Z
- optical1_ctltrc:200201101800:tar.Z
- optical1_ora_arc_incr_backup_200201101800.log

```
ftp> prompt
ftp> mget optical1*200201100200*
ftp> mget optical1*200201101800*
ftp> quit
ls *200201100200*
ls *200201101800*
```

f. Uncompress your files:

```
uncompress *200201100200*.Z
uncompress *200201101800*.Z
```

Note At this point all files are restored from remote ftp server in the */opt/oraback* directory. You are now ready to apply the database recovery processes to bring your database up to the point of your last backup.

Step 7 Clean up old database data files by entering the following commands:

```
cd /data1/oradata/optical1
```

Note If you are on the secondary EMS, cd to /data1/oradata/optical2.

```
rm data/* db1/* db2/* index/*

df -k /data1/oradata
```

Note You must have a minimum of 3.6 GB free disk space on */data1/oradata/optical1* to accommodate all database data files from backup.

Step 8 Restore the backup binary control file to the database target directories:

Use the most current backup binary control file. In this case use the optical1_ctl_binary:200201101800 file from 18:00pm archivelog backup. If archivelog backup was not restored use the binary control file from 2:00am backup. Copy the backup binary control file to both db1/control01.dbf and db2/control02.dbf files.

```
cp /opt/oraback/optical1_ctl_binary:200201101800 db1/control01.ctl
cp /opt/oraback/optical1_ctl_binary:200201101800 db2/control02.ctl
```

Step 9 Recover the database using the **recover_db_until_time.ksh** script.

The **recover_db_until_time.ksh** script uses the restored binary control file to mount the database, restores all data files from the restored database data-sets, applies all applicable archivelog files through the restored archivelog file sets, then finally opens the database with the reset logs option and adds the temp file backup to TEMP tablespace. When this script is completed successfully, database is recovered to the point of time of the backups.

Before executing the recovery_db_until_time.ksh, shut down all Oracle instance processes.

```
cd /opt/oracle/admin/backup
./recover_db_until_time.ksh $ORACLE_SID
```

System response similar to the following is displayed:

```
********************************************************************************
This process will perform database recovery using RMAN backup datasets.

Target: hostname=priems16 database=optical1

You must complete the following procedures before this process:

1. platform stop all
2. stop_cron.sh
3. restore all required backup datasets to /opt/oraback directory
4. copy optical1_ctl_binary file to /data1/../<db1 and db2>

********************************************************************************

Do you want to continue? [y/n] y << Enter y

Log file: /opt/oracle/tmp/recover_db_until_time_200201101636.log

<Thu Jan 10 16:36:51 CST 2002> ./recover_db_until_time.ksh started.
Mounting control file...
Connected to an idle instance.
ORACLE instance started.

Total System Global Area 287912096 bytes
Fixed Size 73888 bytes
Variable Size 181915648 bytes
Database Buffers 104857600 bytes
Redo Buffers 1064960 bytes
Database mounted.

Restoring all datafiles ..
RMAN> 2> 3> 4> 5> 6> 7> 8>
<Thu Jan 10 16:40:15 CST 2002> All datafiles are restored.

<Thu Jan 10 16:40:15 CST 2002> Begin to recover database.

Recover database until time '20020111 14:00:13' << until time is always the restored
timestamp+1day
Last logseq=6782 thread=1

RMAN msglog file: /opt/oracle/tmp/recover_db_until_time_200201101636.log
RMAN> 2> 3> 4> 5> 6> 7> 8>
**** You can Ignore RMAN error messages regarding to: << Ignore this error message from
the log file
**** MAN-08060: unable to find archivelog
**** RMAN-08510: archivelog thread=1 sequence=6783
**** .......
**** RMAN-06054: media recovery requesting unknown log:

<Thu Jan 10 16:44:27 CST 2002> Database recovery ended.

<Thu Jan 10 16:44:27 CST 2002> Alter database open resetlogs
Connected.
Database altered.
….
Database is successfully recovered.
```

```
<Thu Jan 10 16:44:38 CST 2002> ./recover_db_until_time.ksh ended.
```

Post Recovery – Cold Backup

Once you have recovered your database, you need to make a cold backup of the database using the *dbadm –E cold_backup* command. The following tar files will be created from the cold backup script. You need to save a copy of these files to the */opt/oraback* directory. Make sure that the following files are saved to the offsite FTP server.

- /opt/oracle/tmp/optical1_DB_upd.tar.gz
- /opt/oracle/tmp/optical1_ADMIN_upd.tar
- /opt/oracle/tmp/optical1_upd.crontab

Step 1 Log in as **oracle**, or **su – oracle**:

Step 2 Enter the following command:

```
dbadm -E cold_backup
```

Note This process can take more than 10 minutes to complete, depending on the volume of data in the database.

Text similar to the following is displayed:

```
This process performs the following tasks:

1. Shutdown optical1 database on priems09.
2. Backup /opt/oracle/admin directory (except arch dump and log).
3. Cold backup database.
4. Backup oracle crontab file.
5. Startup database.

The following backup files are generated at the end of process:

/opt/oracle/tmp/optical1_DB_upd.tar.gz
/opt/oracle/tmp/optical1_ADMIN_upd.tar
/opt/oracle/tmp/optical1_upd.crontab

Free disk space left on /opt/oracle/tmp: 1383 MB

************************************************************
LOG file: /opt/oracle/tmp/ora_cold_backup.log


Do you want to continue? [y/n] y
```

Step 3 Once the cold backup is completed, save a copy of the backup files to the */opt/oraback* directory for the ftp script to transfer offsite.

```
cd /opt/oracle/tmp
cp optical1_ADMIN_upd.tar /opt/oraback
cp optical1_upd.crontab /opt/oraback
cp optical1_DB_upd.tar.gz /opt/oraback
```

Step 4 Clean up the restored files in */opt/oraback* directory to claim the disk space back.

```
ls /opt/oraback/*200201100200*
ls /opt/oraback/*200201101800*

rm /opt/oraback/*200201100200*
rm /opt/oraback/*200201101800*
```

Step 5 Resume operations.

You are now ready to shut down the Oracle database and start the platform and cron process.

Step 6 Log in as **root** or **su - root**

Step 7 Enter the following commands:

```
su - root
platform stop -i oracle
platform start
svcadm enable svc:/system/cron
nodestat
```

The recovery of the primary EMS database is now complete. To recover the secondary EMS database, copy data from the primary EMS database. Refer to the "Recovering the Element Management System Database from Another Database".

Recovering the Element Management System Database from Another Database

This section provides the procedures to recover one corrupted EMS database from another active database.

Recovery Procedures

The steps in this section show you how to recover a corrupted EMS database from the other active peer database assuming the following scenarios (this procedure applies to both scenarios):

Scenario 1	The primary EMS database is corrupted. You would like to restore data from the secondary EMS database.
Scenario 2	The secondary EMS database is corrupted. You would like to restore data from the primary EMS database.

Step 1 On the active EMS site, terminate the DBHeartBeat process and disable PUSH job (job 2).

a. On the active EMS site, log in as **oracle**, or **su - oracle.**

b. Enter the following command to terminate DBHeartBeat process:

```
$ dbinit -H -i stop

$ ps -ef | grep hbmgr | grep -v grep
```

c. Disable PUSH job (job 2).

```
$ dbadm -A disable_push_job
```

d. Respond **y** at the prompt and enter the following:

```
$ dbadm -r get_broken_jobs
```

Text similar to the following is displayed:

```
2 Y     0   declare rc binary_integer; begin rc := sys.dbms_defer_s
            ys.push(destination=>'OPTICAL1', stop_on_error=>FALSE,
            delay_seconds=>0, parallelism=>1); end;
```

Step 2 Shut down all processes on the corrupted EMS site:

a. On the corrupted EMS site, login as **root**.

b. Stop the cron process and shut down the platform:

```
# svcadm disable svc:/system/cron
# platform stop all
# nodestat

Verify whether all database processes are terminated:
# nodestat
# ps –ef | grep ora_
# ps –ef | grep hbmgr
# ps –ef | grep tnslsnr
```

Tip You can use *kill –9* to kill any process not being terminated by *platform stop all*.

```
# ipcs –p | grep oracle
```

Tip You can use the *ipcrm* command to remove any shared memory or semaphore still allocated to *oracle* now. For example: ipcrm –m <identification (ID)>, ipcrm –s <ID>

Step 3 **This step is optional.** Save all current database logs and trace files on the corrupted EMS site.

If the disk that stores the Oracle database dump and log files still exists, you can save the dump and log files to use later if needed.

a. On the corrupted EMS site, log in as **oracle**, or **su – oracle**:

b. Enter the following commands:

```
$ su - oracle
$ cd /data1/dump
$ tar -cvf /opt/oraback/data1_dump_corrupted.tar *
$ cd /opt/oracle/tmp
$ tar -cvf /opt/oraback/opt_oracle_tmp_corrupted.tar *
```

Timesaver You can gzip or compress the tar files if they are very large.

Step 4 On the corrupted EMS site, rebuild the Oracle database from one of the following three options:

Option 1 If only database is corrupted and the Cisco BTS 10200 Softswitch re-installation is not required, go to Step 5 to reload the database from the database backup file. Continue to Step 6.

Option 2 If the entire system is corrupted and flash archive system backup is available, recover the system from the flash archive, as detailed in the "Flash Archive Restore" section on page 16-2. The flash archive backup file should have the Cisco BTS 10200 Softswitch applications included. Continue to Step 6.

Option 3 If the entire system is corrupted and the flash archive backup file is not available, you must jump start the system, and reinstall the Cisco BTS 10200 Softswitch software from the installation CD, as shown below, Reinstalling the Cisco BTS 10200 Softswitch Software on the Corrupted EMS.

Reinstalling the Cisco BTS 10200 Softswitch Software on the Corrupted EMS

a. Update **/etc/opticall.cfg** file. You can copy this file from active EMS. Verify that the contents are correct.

b. Create the **/opt/ems/utils** directory, if it does not already exist. Enter the following command:

```
# mkdir -p /opt/ems/utils
```

c. FTP the file **/opt/ems/utils/Version** from the active EMS to the corrupted EMS, then rename the file to **Version.save** for reference. Enter the following commands:

```
# cd /opt/ems/utils
# cat Version.save
  900-xx.yy.zz.VVV
```

d. Enter the following commands to create the version file from **Version.save**, but change the version number to D00 (D zero zero). This D00 version value is only a tag; it does not affect the target version to be installed.

```
# sed 's/...$/D00/' Version.save > Version
# cat Version
  900-xx.yy.zz.DOO
```

e. Change to the CD Build directory and run **install.sh** with the -upgrade option. Enter the following command:

```
# ./install.sh -upgrade
```

Note For procedures on how to mount the installation CD and load or untar the software packages to **/opt/Build**, see the following sections in "*Application Installation Procedure (Release 4.4)*":

- "Load the K9-opticall.tar(.gz) File on the EMS and CA/FS Platforms" on page 15
- "Load the K9-oracle.tar(.gz) File on the EMS" on page 23

f. After the corrupted EMS system is reinstalled, enter the commands below to shut down the platform and only start up Oracle listener and database:

```
# platform stop all
# su - oracle
# dbinit -L -E -i start
```

Continue to Step 6.

Step 5 Reload the database from cold backup to the corrupted EMS site.

If the EMS system is intact, but only the Oracle database is corrupted, you can use the cold backup tar file to restore the database data files. The cold backup tar file **optical1_DB_upd.tar.gz** is for the primary EMS, and **optical2_DB_upd.tar.gz** is for the secondary EMS.

- If the tar file is not in **/opt/oraback** directory and the same file still exists in the **/opt/oracle/tmp** directory, copy this file from **/opt/oracle/tmp to /opt/oraback** directory.
- If the file does not exist on either directory, restore this file from remote FTP server to /opt/oraback directory, then execute the steps in this section to restore database data files from the cold backup tar file.

Note If there is no cold backup database tar file, you can restore database from hot backup. Refer to the "Element Management System Database Recovery from Hot Backup" section on page 16-10 to recover your database from hot backup.

a. Restore the database from the cold backup tar file. Log in as **oracle**:

If the corrupted database is the primary EMS database use the ***optical1_DB_upd.tar.gz*** file:

```
$ cd /data1/oradata/optical1
$ rm -r data/* db1/* db2/* index/*
$ gzip -cd /opt/oraback/optical1_DB_upd.tar.gz | tar xvf -
```

If the corrupted database is the secondary EMS database, use the ***optical2_DB_upd.tar.gz*** file:

```
$ cd /data1/oradata/optical2
$ rm -r data/* db1/* db2/* index/*
$ gzip -cd /opt/oraback/optical2_DB_upd.tar.gz | tar xvf -
```

b. Start the database restore process. After the database data files are re-stored, execute the following command to start up the EMS database process:

```
$ dbinit -L -E -i start
```

Step 6 Stop all transactions except northbound traffic on the active EMS. From the active EMS side, stop all transactions to the database except northbound traffic and status control update from CA or FS.

Caution There is no CLI provisioning and Simple Network Management Protocol (SNMP) processes must be stopped.

a. Log in as ***root***.

b. **Enter the following command:**

```
# pkill smg3
```

Step 7 Copy data from the active EMS database to the corrupted database:

Caution During this step the **dbadm -A copy_all** process will truncate local tables first, then copy data from the tables on the other site. ***Make sure that you execute this step on the corrupted EMS side only.***

a. On the corrupted EMS side, log in as **oracle**, or **su – oracle**.

Note Make sure that you are on the corrupted database site.

b. Enter the following command:

```
$ dbadm -A copy_all
```

Text similar to the following is displayed:

```
**************************************************************
You are about to execute the following process:

==> Copy all OAMP/OPTICALL/BILLING tables from remote DB optical1 at priems47

database: optical2
hostname: secems47

**************************************************************
```

c. At the prompt, enter **y** to continue:

```
Do you want to continue? [y/n] y
```

Text similar to the following is displayed:

```
***This will EMPTY all the tables on:
*** local host ==> secems47
*** local database ==> optical2
***
*** Then copy data from remote DB optical1 at priems47
```

d. At the prompt, enter **y** to continue:

```
Do you want to continue? [y/n] y
```

Note This process will take some time. At a database with maximum capacity, it can take approximately 2 hours to copy all operations, administration, maintenance and provisioning (OAMP) and OPTICALL tables.

Response similar to the following example is displayed:

```
<Mon Jan 24 11:40:23 CST 2005> INFO: DMMgr::Configuration loaded
<Mon Jan 24 11:40:23 CST 2005> INFO: DMMgr::243 rows updated
<Mon Jan 24 11:40:24 CST 2005> INFO: DMMgr::Disabling Foreign Key constraints for
BILLING.
<Mon Jan 24 11:40:24 CST 2005> INFO: DMMgr::Disabling triggers for BILLING...
<Mon Jan 24 11:40:25 CST 2005> INFO: copy table => BILLING.BILLING_ACCT_ADDR..
<Mon Jan 24 11:40:26 CST 2005> INFO: copy table => BILLING.BILLING_ACCT_ADDR ...
...
Mon Jan 24 11:40:28 CST 2005> INFO: copy tables => OK=3, FAIL=0, SKIP=0, OTHERS=0
```

```
<Mon Jan 24 11:40:28 CST 2005> INFO: DMMgr::Enabling Foreign Key constraints for
BILLING.
<Mon Jan 24 11:40:28 CST 2005> INFO: DMMgr::Enabling triggers for BILLING...
<Mon Jan 24 11:40:29 CST 2005> INFO: DMMgr::Disabling Foreign Key constraints fo
r OAMP...
<Mon Jan 24 11:40:29 CST 2005> INFO: DMMgr::Disabling triggers for OAMP...
<Mon Jan 24 11:40:29 CST 2005> INFO: copy table => OAMP.CALL_TRACE..
<Mon Jan 24 11:40:30 CST 2005> INFO: copy table => OAMP.CALL_TRACE ...OK(0 row)
...
<Mon Jan 24 11:41:41 CST 2005> INFO: copy tables => OK=50, FAIL=0, SKIP=0, OTHER
S=0
<Mon Jan 24 11:41:41 CST 2005> INFO: DMMgr::Enabling Foreign Key constraints for
OAMP...
<Mon Jan 24 11:41:41 CST 2005> INFO: DMMgr::Enabling triggers for OAMP...
<Mon Jan 24 11:41:41 CST 2005> INFO: DMMgr::Disabling Foreign Key constraints for
OPTICALL…
<Mon Jan 24 11:42:07 CST 2005> INFO: DMMgr::Disabling triggers for OPTICALL...
<Mon Jan 24 11:42:47 CST 2005> INFO: copy table => OPTICALL.AAA_SERVER_GRP..
<Mon Jan 24 11:42:48 CST 2005> INFO: copy table => OPTICALL.AAA_SERVER_GRP ...OK (0
row)
...
Mon Jan 24 11:46:41 CST 2005> INFO: copy table => OPTICALL.WIRETAP..
<Mon Jan 24 11:46:42 CST 2005> INFO: copy table => OPTICALL.WIRETAP ...OK(0 row)
<Mon Jan 24 11:46:42 CST 2005> INFO: copy tables => OK=190, FAIL=0, SKIP=0, OTHERS=0
<Mon Jan 24 11:46:42 CST 2005> INFO: DMMgr::Enabling Foreign Key constraints for
OPTICALL...
<Mon Jan 24 11:47:20 CST 2005> INFO: DMMgr::Enabling triggers for OPTICALL...
```

Step 8 On the active EMS, truncate all replication queues since all data are already copied over, then start the DBHeartBeat process. The DBHeartBeat process automatically enables the broken push job.

From active EMS side:

a. Truncate replication queues. Enter the following commands:

```
# su - oracle

$ dbadm -A truncate_def

$ dbadm -r get_unpushed_trans
```

Text similar to the following is displayed:

```
no rows selected
```

b. Start the DBHeartBeat process. Enter the following command:

```
$ dbinit -H -i start

$ dbadm -r get_broken_jobs
```

Text similar to the following is displayed:

```
2 N          0           declare rc binary_integer; begin rc :=
sys.dbms_defer_sys.push(destination=>'OPTICAL1',
stop_on_error=>FALSE,delay_seconds=>0, parallelism=>1); end;
```

Step 9 Verify the database status and audit contents of tables. This step can be executed on either the primary or secondary EMS site. In this case, it is executed on the primary EMS site.

a. On the active EMS site, log in as **oracle**, or **su - oracle**.

b. Enter the following command:

```
$ dbadm -C db
```

Response similar the following example is displayed:

```
OPTICAL1::Deftrandest is empty?              YES

OPTICAL1::dba_repcatlog is empty?            YES

OPTICAL1::Deferror is empty?                 YES

OPTICAL1::Deftran is empty?                  YES

OPTICAL1::Has no broken job?                 YES

OPTICAL1::JQ Lock is empty?                  YES


OPTICAL2::Deftrandest is empty?              YES

OPTICAL2::dba_repcatlog is empty?            YES

OPTICAL2::Deferror is empty?                 YES

OPTICAL2::Deftran is empty?                  YES

OPTICAL2::Has no broken job?                 YES

OPTICAL2::JQ Lock is empty?                  YES


    Checking table => OPTICALL.AGGR....OK
        Checking table => OPTICALL.ANI....OK
        ..
        ..

        Number of tables to be checked: xxx
        Number of tables checked OK: xxx
        Number of tables out-of-sync: 0
```

Step 10 Synchronize table contents from the uncorrupted EMS site to the corrupted EMS site.

If the dbadm -C db command from Step 9 returns out-of-sync table(s) like the examples below, follow the commands in Step a. and Step b. (below) to synchronize the contents of data from the active EMS database to the corrupted EMS database.

Text similar to the following example is displayed:

```
Number of tables to be checked: 130
Number of tables checked OK: 127
Number of tables out-of-sync: 3
```

List of out of sync tables:

```
OAMP.TABLE_NAME => 22/0
```

In this example, one table owned by the OAMP is out of sync. Follow the steps below to synchronize the contents of the tables:

Note Execute these commands on the corrupted EMS database to synchronize the table.

Truncate the content of the table on the local database, then copy the data from the remote database, as follows:

a. Log in as **oracle**, or **su - oracle**:

b. Enter the following commands:

```
$ dbadm -A copy -o <owner> -t <table_name>

$ dbadm -A copy -o oamp -t table_name
```

Step 11 Verify the Oracle crontab file:

a. Log in as **oracle**, or **su - oracle**:

b. Verify the Oracle crontab file on the corrupted EMS site. Compare the schedules of jobs with those on the active EMS site. If any schedule needs to be modified, enter the following command:

```
$ crontab -e
```

Step 12 Shut down the Oracle database and start up the platform on the standby EMS sites. Both primary and secondary databases have identical data. You must start the platform and system cron processes on the standby EMS.

On the corrupted EMS site, log in as **root** and enter the following commands to bring up the platform:

```
# su - oracle
$ dbstat -a -f
$ dbstat -j bts10200_bts_stat_daily -J enable -f
$ dbadm -s get_dbms_schedules | grep -i stat_daily | grep -i gather_bts
    BTS10200_BTS_STAT_DAILY BTS10200_GATHER_BTS SCHEDULED TRUE
$ exit
# platform stop -i oracle
# platform start
# svcadm enable svc:/system/cron

# su - oracle

$ dbadm -A stat_bts_job
```

The EMS database recovery from another database is now complete.

Fresh Download

The Fresh Download command refreshes data in Call Agent shared memory. It recovers the data in the Call Agent shared memory in the event that shared memory data cannot be recovered by any other means. The fresh download wipes out Call Agent shared memory data and causes a total outage.

Caution Do not use this command on **any** live traffic production systems. Please contact Cisco TAC regarding the use of this command for disaster recovery.

You can perform the command by ID. The download by ID command allows you to copy database information from the EMS to a specific CA or FS. If a CA ID is not specified, the command copies to all IDs.

Use one of the following examples to perform a fresh download by ID.

```
download database target=ca; id=CA146
download database target=fsptc; id=FSPTC135
download database target= fsain; id=FSAIN125
```

See the *Cisco BTS 10200 Softswitch Command Line Interface Reference Guide* for table and token descriptions.

Call Agent Database Download and Recovery

This call agent database download and recovery procedure is recommended as a last resort for recovering corrupted call agent databases.

Note Please contact Cisco TAC regarding the use of this procedure for call agent database recovery.

Note If transactions are stuck in the queue, execute a **delete transaction-queue** CLI command before beginning this procedure.

Step 1 Execute the following **download database** CLI commands.

```
CLI> download database target=ca; file=/opt/tmp/download-CA
CLI> download database target=fsain; file=/opt/tmp/download-FSAIN
CLI> download database target=fsptc; file=/opt/tmp/download-FSPTC
```

Step 2 Perform a **platform stop all** command on both call agents.

Step 3 Delete the following data directories on the primary and secondary call agents.

```
cd /opt/OptiCall
\rm -rf */bin/data
```

Step 4 Start the primary call agents or feature servers with the **platform start** command.

Step 5 FTP the files created in Step 1 to the primary call agent.

```
download-CA -ftp to-> /opt/OptiCall/CAxxx/bin
download-FSPTC -ftp to-> /opt/OptiCall/FSPTxxx/bin
download-FSAIN205 -ftp to-> /opt/OptiCall/FSAINxxx/bin
```

Step 6 Go into mysql on the primary call agent or feature server and upload the database as shown. This is to be done in parallel with three different sessions opened to the appropriate call agent or feature server.

a. From the /opt/OptiCall/CAxxx/bin command line:

```
./dbm_sql.CAxxx ./data ./catalog < download-CA
```

b. From the /opt/OptiCall/FSPTCxxx/bin command line:

```
./dbm_sql.FSPTCxxx ./data ./catalog < download-FSPTC
```

c. From /opt/OptiCall/FSAINxxx/bin command line:

```
./dbm_sql.FSAINxxx ./data ./catalog < download-FSAIN
```

Step 7 Start the secondary call agents or feature servers with the **platform start** command.

Step 8 Control all provisioned network devices to in service using manually generated return to service scripts.

Note The following steps should be run in parallel to limit the amount of down time; for example, one engineer working on returning subscribers to in service and one engineer working on returning trunks, trunk-grps, and so forth to in service.

a. Complete the following items with scripts manually created through CLI.

```
- control trunks oos
- control trunk-grps oos
- control h323gws oos
- unequip trunk terminations
- control h323gws ins
- control trunk-grps ins
- equip trunk terminations
- control trunks ins
```

b. Bring subscribers into service utilizing the cs-control tool. A script is generated with all the subscriber terminations. An example of the script is as follows:

```
control subscriber-termination id=sub1; mode=forced; target-state=INS
control subscriber-termination id=sub2; mode=forced; target-state=INS
control subscriber-termination id=sub3; mode=forced; target-state=INS
control subscriber-termination id=sub4; mode=forced; target-state=INS
```

c. Place the completed script in the /opt/OptiCall/CAxxx/bin directory on the primary call agent.

d. Invoke the cs-control script from /opt/OptiCall/CAxxx/bin directory to place subscribers in service.

```
cs-control data <name of script from step 8b>
```

Recovering Shared Memory Data

The **download database** command refreshes data in the Call Agent (CA) shared memory. In the event that shared memory data cannot be recovered, it recovers data in the CA shared memory. The **download database** command wipes out Call Agent shared memory data and causes a total outage.

Caution **Read this section in its entirety before attempting this procedure.**

Do not use this command on **any** live traffic production systems. Contact Cisco TAC regarding the use of this command for disaster recovery.

Caution Do not download the database through the console port because the TTY can cause long delays.

Downloads of the CA, FSAIN and FSPTC applications can be done in parallel.

You can perform the **download database** command by ID. The download by ID command allows you to copy database information from the EMS to a specific CA or Feature Server (FS). If a CA ID is not specified, the command copies to all IDs.

Use one of the following examples to download database by ID.

```
download database target=ca; id=CAxxx
download database target=fsptc; id=FSPTCxxx
download database target= fsain; id=FSAINxxx
```

See the *Cisco BTS 10200 Softswitch Command Line Interface Reference Guide* for table and token descriptions.

Recovering Shared Memory

Perform the following procedure:

Step 1 Check the transaction queue. Use the following command:

```
show transaction-queue
```

Step 2 If you find any transaction in the queue, delete the queue by entering the following CLI command.

Note There should be no provisioning activity on the system—if the **show transaction-queue** command does not return the message "Void of entries," assume that a transaction is in the queue. If there is no transaction in the queue, proceed to Step 7

delete transaction-queue target=*CAxxx;* **transaction-id**=*<id>*

The **transaction-id** parameter enables you to delete only one transaction at a time from the transaction_queue table. Note that to delete an entry from the transaction-queue, you should login as **ciscouser**.

Examples:

delete transaction-queue target=CAxxx; **transaction-id=***<id>*

```
delete transaction-queue target=FSPTCxxx; transaction-id=<id>
delete transaction-queue target=FSAINxxx transaction-id=<id>
```

If there are thousands of entries stuck in the transaction queue, it is recommended to flush all the entries from Oracle after logging in as **oamp** user.

Perform the following steps to login as **oamp** user and to flush all the entries from Oracle:

Step 1 `<hostname># su - oracle`

Step 2 `<hostname>$ sqlplus oamp/oamp`

Step 3 `SQL> delete from transaction_queue;`

Step 4 `SQL> commit;`

Step 5 `SQL> exit`

Step 6 `<hostname>$ exit`

In the following example, 138327 transactions are stuck in the queue, and the display of the transactions (using the **show** command) is limited to 2. This example shows that when many transactions are stuck in the queue, deleting one transaction at a time takes huge amount of time. In such scenarios, it is recommended to flush all the entries from Oracle.

```
CLI> show transaction_queue limit=2

TRANSACTION_ID=1242510999092
SEQUENCE_NUM=0
TARGET=CA101
STATEMENT=delete from MGW_PROFILE;
TIMESTAMP=2009-05-16 17:26:39
ACTIVE_TARGET=Y
USERNAME=null
TERMINAL=null
STATUS=FAILED

TRANSACTION_ID=1242510999092
SEQUENCE_NUM=1
TARGET=CA101
STATEMENT=delete from NDC;
TIMESTAMP=2009-05-16 17:26:39
ACTIVE_TARGET=Y
USERNAME=null
TERMINAL=null
STATUS=PENDING

Reply : Success:  Entries 1-2 of 138327 returned.
```

If you want to delete the first transaction, enter the following command:

```
CLI> delete transaction_queue target=CA101;transaction_id=1242510999092;
Reply : Success: CLI delete successfully
```

Step 7 Enter the shared memory command to recover the CA and FS databases. Enter following CLI download database commands:

```
download database target=CA; file=/tmp/download-CA
download database target=FSAIN; file=/tmp/download-FSAIN
download database target=FSPTC; file=/tmp/download-FSPTC
```

Step 8 Stop both CA platforms. Enter the following command:

```
platform stop all
```

Step 9 Delete the following data directories (as shown below) on the primary and secondary CA and FSs. Enter the following commands:

```
cd /opt/OptiCall
\rm -rf */bin/data
```

Step 10 Use ftp to transfer the file created in Step 7 to the primary CA. Place the files in the following directories:

```
download-CA in /opt/OptiCall/CAxxx/bin
download-FSPTC in /opt/OptiCall/FSPTCxxx/bin
download-FSAIN in /opt/OptiCall/FSAINxxx/bin
```

Step 11 Start the primary CA and FS platforms. Enter the following command:

```
platform start
```

Step 12 Upload the database files using the dbm_dql tool as shown below.

Note Perform this step in parallel with three different sessions opened to the appropriate CA or FS.

The following steps may take up to 2 hours, depending on the size of the database being recovered.

a. Enter the following from the /opt/OptiCall/CAxxx/bin command line:

```
/dbm_sql.CAxxx ./data ./catalog < download-CA
```

b. Enter the following from /opt/OptiCall/FSPTCxxx/bin command line:

```
/dbm_sql.FSPTCxxx ./data ./catalog < download-FSPTC
```

c. Enter the following from /opt/OptiCall/FSAINxxx/bin command line:

```
/dbm_sql.FSAINxxx ./data ./catalog < download-FSAIN
```

Step 13 Start the secondary CA and FS platforms after Step 12 completes.

```
platform start
```

Step 14 Continue to the following procedure, Restoring Subscriber and Trunk Terminations to Service.

Restoring Subscriber and Trunk Terminations to Service

Control all provisioned network devices in service, as shown in the following subsections.

Caution You must run the following procedures in parallel, to limit the amount of down time. For example, one engineer can be working on subscribers while another engineer is working on trunks or trunk groups.

Controlling Trunks and Trunk Groups

Control trunks and trunk groups with scripts created through the following CLI commands:

CLI Command	Example
control trunks oos	control trunk-termination tgn-id=1;cic=1-24;mode=forced; target-state=oos;
control trunk-grps oos	control trunk-grp id=1;mode=forced;target-state=oos;
control h323gws oos	control h323-gw id=h323;mode=forced;target-state=oos;
unequip trunk terminations	unequip trunk-termination tgn-id=1;cic=all;
control h323gws ins	control h323-gw id=h323;mode=forced;target-state=ins;
control trunk-grps ins	`control trunk-grp id=1;mode=forced;target-state=ins;`
`equip trunk terminations`	`equip trunk-termination tgn-id=1;cic=all;`
`control trunks ins`	`control trunk-termination tgn-id=1;cic=1-24;mode=forced;target-state=ins;`

Using the cs-control Tool to Bring Subscribers In-Service

Use the cs-control tool to bring subscribers in-service. Obtain the cs-control tool from Cisco. You must write a script (as shown in the following example) to be used by the cs-control tool.

Example of a Script

```
control subscriber-termination id=sub1;mode=forced;target-state=INS
control subscriber-termination id=sub2;mode=forced;target-state=INS
control subscriber-termination id=sub3;mode=forced;target-state=INS
control subscriber-termination id=sub4;mode=forced;target-state=INS
```

Note The completed script will be placed in the /opt/OptiCall/CAxxx/bin directory on the primary CA.

The cs-control script is invoked from /opt/OptiCall/CAxxx/bin directory to place subscribers in-service as follows:

`cs-control data <name of the script used in the step above>`

Disaster Recovery Using the Automatic Shared Memory Backup

Note This procedure is for use with Cisco BTS 10200 Softswitch Release 4.5.1 and above.

The purpose of the section is to describe the procedure for restoring a BTS network element's shared memory from a backup copy created by the BTS Automatic Shared Memory Backup subsystem.

This procedure should **only** be run in the event of corrupted shared memory in both the Active and Standby side of the same BTS network element (NE).

Note There is an existing procedure that achieves this same end result. However, it requires a download from the EMS, which can take a relatively long time to complete. The advantage of using the procedure listed here is that the EMS is bypassed, allowing the Call Agent or Feature Server platform to be restored to an operational state in a much shorter time

Additionally, note that the data in the Automatic Shared Memory Backup (ASMB) can be up to 24 hours old. Provisioning done in the time since the backup will be restored only after an audit and sync with the EMS is completed at the end of the procedure.

Before You Begin

This procedure should only be completed if both of the following conditions are true:

- Both Side A and Side B of the same Cisco BTS 10200 Softswitch network element are out of service.
- Neither side of the same Cisco BTS 10200 Softswitch network element can be returned to service with a **platform start** command due to corrupted shared memory

If these conditions are true, then the Cisco BTS 10200 Softswitch network element should be restored to the ASMB backup copy of the shared memory. **If not, then do not perform this procedure.**

Before restoring your system, you must have the following:

- Console access to the system to be restored
- Location of the ASMB shared memory backup for the platform. This backup resides on the system in the /bin directory of each Cisco BTS 10200 Softswitch network element.

Automatic Shared Memory Backup Restore

This section describes the procedure for restoring a platform to its ASMB shared memory backup.

It is possible that multiple Cisco BTS 10200 Softswitch network elements (NEs) need to have the shared memory restored. If so, then this procedure should be executed for each one. It is recommended that the NEs be recovered (if necessary) in the following order:

- Call Agent (CA)
- Feature Server – POTS
- Feature Server – AIN
- Element Management System (EMS)
- Billing Data Management System (BDMS)

The EMS and BDMS are usually hosted on a separate system from the Call Agent and Feature Servers, therefore they can be recovered in parallel with the NEs on the CA/FS system.

Additionally, all BTS NEs on one of the systems should be restored first before attempting to restore the ones on the mate. This will ensure that full service is restored as soon as possible.

Step 1 Use the console to gain access to Side A and Side B of the system with the network element(s) to be restored.

Step 2 Verify that both Side A and Side B of the NE are out of service using the **nodestat** command. Verify neither NE will return to service after a **platform start** command. If either side is in service or can be returned to service, exit this procedure.

Step 3 Choose which side of the NE to restore first. We recommend Side A as a convention, and therefore will refer to Side A in this procedure. Exit from the console of the other system.

Step 4 On Side A, run the script **restoreSharedMemory**. This script will remove the current, corrupted shared memory and then replace it with the ASMB backup copy. To restore the call-agent, run **restoreSharedMemory -i CAxxx**.

Step 5 Bring the Cisco BTS 10200 Softswitch NE back into service with the **platform start** command.

Step 6 Verify that the NE returns to service in the Active state using the **nodestat** command.

Step 7 Repeat Step 4 to Step 6 for FSPTC and FSAIN if necessary using **restoreSharedMemory -i FSPTCyyy** and **restoreSharedMemory -i FSAINzzz**.

Step 8 After all Cisco BTS 10200 Softswitch NEs are in service on Side A, perform an **Audit** of the EMS system database to the CA/FS system database. The Audit will report any differences between the two system databases. Because the data in the CA/FS shared memory backup can be up to 24 hours old, it is likely there will be differences. These should then be resolved with a **Sync** of the EMS database to the CA/FS database.

Step 9 Perform some test calls to verify that full functionality is provided by the Cisco BTS 10200 Softswitch after all NEs on Side A have been completely restored. If there are any problems, contact Cisco TAC immediately.

Step 10 Next, the mate Side B network elements that are out of service need to be restored. For each network element that needs to be restored on Side B, remove its shared memory directory (/../bin/data) using the unix **rm** command. This should only be done for network elements that are out of service. Start the down NE(s) with the **platform start** command. The network element(s) will start and copy the shared memory database from their Active Side A network element mate(s).

Step 11 Verify that the mate Side B network elements have all returned to service in the Standby state using the **nodestat** command.

Restore Shared Memory Script

This section describes actions performed by the **restoreSharedMemory** script. The **restoreSharedMemory** script completes these actions automatically. These steps do not need to be performed by the user as part of the recovery procedure.

Step 1 Verifies that the platform is OOS-FAULTY. This procedure should not be run otherwise.

Step 2 Verifies that the installed software version matches the software version of the ASMB shared memory backup copy to be used. The ASMB backup has the software version and timestamp in its name. For example: **data.bak.900-04.05.01.V14.2006_08_29__02_00_06**

Step 3 Renames the current, corrupted shared memory data directory to keep for potential offline debugging. The software version and the current time are used in the name. For example: **data.corrupt.900-04.05.01.V14.2006_09_01__00_21_50**

Step 4 Copies the most recent ASMB shared memory backup copy to the **data** directory for the Cisco BTS 10200 Softswitch NE being restored.

CHAPTER 17

Disk Replacement

Revised: July 22, 2009, OL-8000-32

Introduction

This chapter describes the process of replacing a defective Cisco BTS 10200 Softswitch disk. Each Cisco BTS 10200 Softswitch system element contains two hard disks (disk 0 and disk 1) that are mirrored using Sun Solaris Disk Suite. The disk mirroring application must be disabled between the two disks in order to replace the defective disk.

Before starting the disk replacement procedures, the following procedures must be completed:

- Identify the disk that needs to be replaced by viewing the **/var/adm/messages**
- Cisco recommends that the new disk part number must be the same as the defective disk or the size of the replacement disk must be equal or larger than the good disk.
- Perform a full system backup procedure.

This chapter contains the following sections:

- Full System Backup Procedure
- Call Agent/Feature Server or Element Management System Disk 0 Replacement
- Call Agent/Feature Server or Element Management System Disk 1 Replacement

Full System Backup Procedure

The purpose of this section is to describe the needed steps to create a backup using the Flash Archive on Cisco BTS 10200 Softswitch system. The procedure is performed before and after any software upgrade or for routine maintenance purposes.

Note It is recommended that this procedure be performed during a maintenance window or when traffic volume is low.

Before you start the backup procedure, obtain the following information:

- NFS server hostname or IP address.
- Shared directory from NFS server.
- Root user access.

Note Provisioning is not allowed during this procedure in order to have a stable backup.

Call Agent/Feature Server Backup

Perform the following steps on STANDBY CA/FS system.

Step 1 Login as root on secondary CA/FS.

Step 2 Verify that all platforms are in STANDBY mode.

<hostname>**#nodestat**

Step 3 Remove all unnecessary files or directories such as: **/opt/Build**, application **tar** files, etc…

Step 4 Mount NFS server to **/mnt** directory.

<hostname>**#mount <nfs server ip or hostname>:/<share dire> /mnt**

Step 5 Stop all platforms.

<hostname>**#platform stop all**

Step 6 Save all platforms data directory (shared memory) to nfs server.

<hostname>**#tar –cf - /opt/OptiCall/CAxxx/bin/data |gzip –fast - > /mnt/data.<hostname>.CA**

<hostname>**#tar –cf - /opt/OptiCall/FSAINxxx/bin/data |gzip –fast - > /mnt/data.<hostname>.FSAIN**

<hostname>**#tar –cf /opt/OptiCall/FSPTCxxx/bin/data |gzip –fast - > /mnt/data.<hostname>.FSPTC**

Note Where **xxx** is the instance number.

Step 7 Start all platforms.

<hostname>**#platform start -nocopy**

Step 8 Verify all platforms are up on STANDBY.

<hostname>**#nodestat**

Step 9 Create excluded directories file for flash archive.

<hostname>**#vi /tmp/excluded_dir**

Add the following lines and save the file:

/opt/OptiCall/CAxxx/bin/data

/opt/OptiCall/CAxxx/bin/logs

/opt/OptiCall/FSAINxxx/bin/data

/opt/OptiCall/FSAINxxx/bin/logs

/opt/OptiCall/FSPTCxxx/bin/data

/opt/OptiCall/FSPTCxxx/bin/logs

Note Where **xxx** is the instance number.

Step 10 Backup the system.

<hostname>**#mv /bin/date /bin/date.archive**

<hostname>**#mv /bin/.date /bin/date**

<hostname>**#flarcreate –n <hostname> -I -X /tmp/excluded_dir –c /mnt/<hostname>.archive**

<hostname>**#mv /bin/date /bin/.date**

<hostname>**#mv /bin/date.archive /bin/date**

Step 11 Un-mount NFS server.

<hostname>**#umount /mnt**

Step 12 Swithover all platforms.

Perform the following commands from the **Active-EMS**.

<hostname>**#ssh optiuser@<hostname>**

cli>control feature-server id=FSAINxxx;target-state=standby-active;

cli>control feature-server id=FSPTCxxx;target-state=standby-active;

cli>control call-agent id=CAxxx;target-state=standby-active;

Note Where **xxx** is the instance number of each platform.

Step 13 Repeat the same steps for the PRIMARY CA/FS.

Element Management System/Bulk Data Management System Backup

Perform the following steps on STANDBY EMS/BDMS system.

Step 1 Remove all unnecessary files or directories such as: **/opt/Build**, application **tar** files, etc…

Step 2 Mount NFS server to **/mnt directory**.

<hostname>**#mount <nfs server ip or hostname>:/<share dire> /mnt**

Step 3 Stop all platforms.

<hostname>**#platform stop all**

Step 4 Save Oracle database and msql directories.

<hostname>**#tar –cf - /data1/oradata |gzip –fast - >/mnt/oradata.<hostname>**

Step 5 Create excluded directories file for flash archive.

<hostname>**#vi /tmp/excluded_dir/data1/oradata**

Step 6 Start all platforms.

<hostname>**#platform start -nocopy**

Step 7 Verify all platforms are up on STANDBY.

<hostname>**#nodestat**

Step 8 Backup the system.

<hostname>**#mv /bin/date /bin/date.archive**

<hostname>**#mv /bin/.date /bin/date**

<hostname>**#flarcreate –n <hostname> -I -X /tmp/excluded_dir –c /mnt/<hostname>.archive**

<hostname>**#mv /bin/date /bin/.date**

<hostname>**#mv /bin/date.archive /bin/date**

Step 9 Un-mount NFS server.

<hostname>**#umount /mnt**

Step 10 Switchover all platforms.

Perform the following commands from the **Active-EMS**.

<hostname>**#ssh optiuser@<hostname>**

cli>control bdms id=BDMS01;target-state=standby-active;

cli>control element-manager id=EM01;target-state=standby-active;

Step 11 Repeat the same steps for PRIMARY EMS/BDMS.

Call Agent/Feature Server or Element Management System Disk 0 Replacement

Note The letter "x" in cxt0d0 or cxt1d0 throughout the procedure is referring to the SCSI controller ID of the system (either 0 or 1). To find out the controller ID, use the **format** command.

Step 1 Login as root.

Step 2 Verify application status.

```
<hostname>#nodestat
```

Note If all platforms on this node are ACTIVE, then you need to switchover to STANDBY side using the CLI command.

Step 3 Stop all BTS 10200 platforms.

```
<hostname>#platform stop all
```

Step 4 Perform the following commands to detach all submirror metadevice.

```
<hostname>#metadetach -f d2 d0
<hostname>#metadetach -f d14 d12
<hostname>#metadetach -f d11 d9
<hostname>#metadetach -f d5 d3
<hostname>#metadetach -f d8 d6
```

Step 5 Perform the following commands to clear all submirror metadevice.

```
<hostname>#metaclear d0
<hostname>#metaclear d12
<hostname>#metaclear d9
<hostname>#metaclear d3
<hostname>#metaclear d6
```

Step 6 Delete database replica on defective disk.

```
<hostname>#metadb -d -f /dev/dsk/cxt0d0s4
```

Step 7 Verify that there is no existing metadevice on defective disk.

```
<hostname>#metastat -p |grep cxt0d0
```

Step 8 Use the **cfgadm** command to determine the defective disk parameter.

Example:

```
secca38#cfgadm -al
```

Ap_Id	Type	Receptacle	Occupant	Condition
c0	scsi-bus	connected	configured	unknown
c0::dsk/c0t0d0	CD-ROM	connected	configured	unknown
c1	scsi-bus	connected	configured	unknown
c1::dsk/c1t0d0	disk	connected	**configured**	unknown
c1::dsk/c1t1d0	disk	connected	configured	unknown
c2	scsi-bus	connected	unconfigured	unknown
usb0/1	unknown	empty	unconfigured	ok
usb0/2	unknown	empty	unconfigured	ok

Step 9 Take disk 0 offline.

```
<hostname>#cfgadm -c unconfigure c1::dsk/cxt0d0
```

Example:

```
Secca38#cfgadm -c unconfigure c1::dsk/c1t0d0
```

Step 10 Verify that Disk 0 is offline.

Example:

```
secca38#cfgadm -al
```

Ap_Id	Type	Receptacle	Occupant	Condition
c0	scsi-bus	connected	configured	unknown
c0::dsk/c0t0d0	CD-ROM	connected	configured	unknown
c1	scsi-bus	connected	configured	unknown
c1::dsk/c1t0d0	disk	connected	**unconfigured**	unknown
c1::dsk/c1t1d0	disk	connected	configured	unknown
c2	scsi-bus	connected	unconfigured	unknown
usb0/1	unknown	empty	unconfigured	ok
usb0/2	unknown	empty	unconfigured	ok

```
secca38#tail /var/adm/messages

Nov  2 15:53:25 secca38 genunix: [ID 408114 kern.info] /pci@1f,700000/scsi@2/sd@0,0 (sd0)
offline
```

Step 11 Remove the defective disk and insert the new replacement disk into slot 0.

Step 12 Use the **cfgadm** command to bring the new Disk 0 on line.

```
<hostname># cfgadm -c configure c1::dsk/cxt0d0
```

Example:

```
Secca38#cfgadm -c configure c1::dsk/c1t0d0
```

Step 13 Verify that the new Disk 0 is on line.

```
<hostname>#cfgadm -al
```

Example:

```
secca38#cfgadm -al

Ap_Id           Type      Receptacle  Occupant      Condition
c0              scsi-bus  connected   configured    unknown
c0::dsk/c0t0d0  CD-ROM    connected   configured    unknown
c1              scsi-bus  connected   configured    unknown
c1::dsk/c1t0d0  disk      connected   configured    unknown
c1::dsk/c1t1d0  disk      connected   configured    unknown
c2              scsi-bus  connected   unconfigured  unknown
usb0/1          unknown   empty       unconfigured  ok
usb0/2          unknown   empty       unconfigured  ok


secca38#tail /var/adm/messages

Nov  2 15:53:25 secca38 genunix: [ID 408114 kern.info] /pci@1f,700000/scsi@2/sd@0,0 (sd0)
online
```

Step 14 Use the **format** and **prtvtoc** commands to partition the new disk

Disk layout:

```
Slice 0 /(root)2000MB
Slice 1 /var 5000MB
Slice 3 swap 4000MB
Slice 4 unassigned 24MB
Slice 5 /opt The rest of the disk space
Slice 6 unassigned 2000MB
```

Step 15 Create the database replica on the new disk.

```
<hostname>#metadb -a -f -c 3 /dev/dsk/cxt0d0s4
```

Step 16 Perform the following commands to create submirror metadevice.

```
<hostname>#metainit -f d0 1 1 /dev/dsk/cxt0d0s0
<hostname>#metainit -f d12 1 1 /dev/dsk/cxt0d0s6
<hostname>#metainit -f d9 1 1 /dev/dsk/cxt0d0s5
<hostname>#metainit -f d3 1 1 /dev/dsk/cxt0d0s1
<hostname>#metainit -f d6 1 1 /dev/dsk/cxt0d0s3
```

Step 17 Install the boot block on the new disk.

```
<hostname>#installboot /usr/platform/`uname -i`/lib/fs/ufs/bootblk /dev/rdsk/cxt0d0s0
```

Step 18 Sync Disk 0 (new disk) with Disk 1.

```
<hostname># metattach d2 d0
<hostname>#metattach d14 d12
<hostname>#metattach d11 d9
<hostname>#metattach d5 d3
<hostname>#metattach d8 d6
```

Note The disk sync process with take awhile depending on the disk size. To find out the percentage completion of this process, you can run the **metastat|grep %** command.

Step 19 Start all BTS 10200 platforms.

```
<hostname>#platform start -nocopy
```

Call Agent/Feature Server or Element Management System Disk 1 Replacement

Note The letter "x" in cxt0d0 or cxt1d0 throughout the procedure is referring to the SCSI controller ID of the system (either 0 or 1). To find out the controller ID, use the **format** command.

Step 1 Login as root.

Step 2 Verify application status.

```
<hostname>#nodestat
```

Note If all platforms on this node are ACTIVE, then you need to switchover to STANDBY side using the CLI command.

Step 3 Stop all BTS 10200 platforms.

```
<hostname>#platform stop all
```

Step 4 Perform the following commands to detach all submirror metadevice.

```
<hostname>#metadetach -f d2 d1
<hostname>#metadetach -f d14 d13
<hostname>#metadetach -f d11 d10
<hostname>#metadetach -f d5 d4
<hostname>#metadetach -f d8 d7
```

Step 5 Perform the following commands to clear all submirror metadevice.

```
<hostname>#metaclear d1
<hostname>#metaclear d13
<hostname>#metaclear d10
<hostname>#metaclear d4
<hostname>#metaclear d7
```

Step 6 Delete database replica on defective disk.

```
<hostname>#metadb -d -f /dev/dsk/cxt1d0s4
```

Step 7 Verify that there is no existing metadevice on defective disk.

```
<hostname>#metastat -p |grep cxt1d0
```

Step 8 Use the **cfgadm** command to determine the defective disk parameter.

Example:

```
secca38#cfgadm -al

Ap_Id           Type      Receptacle  Occupant      Condition
c0              scsi-bus  connected   configured    unknown
c0::dsk/c0t0d0  CD-ROM    connected   configured    unknown
c1              scsi-bus  connected   configured    unknown
c1::dsk/c1t0d0  disk      connected   configured    unknown
c1::dsk/c1t1d0  disk      connected   configured    unknown
c2              scsi-bus  connected   unconfigured  unknown
usb0/1          unknown   empty       unconfigured  ok
usb0/2          unknown   empty       unconfigured  ok
```

Step 9 Take disk 1 offline.

```
<hostname>#cfgadm -c unconfigure c1::dsk/cxt1d0
```

Example:

```
Secca38#cfgadm -c unconfigure c1::dsk/c1t1d0
```

Step 10 Verify that Disk 1 is offline.

Example:

```
secca38#cfgadm -al

Ap_Id           Type      Receptacle  Occupant      Condition
c0              scsi-bus  connected   configured    unknown
c0::dsk/c0t0d0  CD-ROM    connected   configured    unknown
c1              scsi-bus  connected   configured    unknown
c1::dsk/c1t0d0  disk      connected   configured    unknown
c1::dsk/c1t1d0  disk      connected   unconfigured  unknown
c2              scsi-bus  connected   unconfigured  unknown
usb0/1          unknown   empty       unconfigured  ok
usb0/2          unknown   empty       unconfigured  ok


secca38#tail /var/adm/messages

Nov  2 15:53:25 secca38 genunix: [ID 408114 kern.info] /pci@1f,700000/scsi@2/sd@0,1 (sd1)
offline
```

Step 11 Remove the defective disk and insert the new replacement disk into slot 1.

Step 12 Use the **cfgadm** command to bring the new Disk 1 on line.

```
<hostname># cfgadm -c configure c1::dsk/cxt1d0
```

Example:

```
Secca38#cfgadm -c configure c1::dsk/c1t1d0
```

Step 13 Verify that the new Disk 0 is on line.

```
<hostname>#cfgadm -al
```

Example:

```
secca38#cfgadm -al

Ap_Id           Type      Receptacle  Occupant      Condition
c0              scsi-bus  connected   configured    unknown
c0::dsk/c0t0d0  CD-ROM    connected   configured    unknown
c1              scsi-bus  connected   configured    unknown
c1::dsk/c1t0d0  disk      connected   configured    unknown
c1::dsk/c1t1d0  disk      connected   configured    unknown
c2              scsi-bus  connected   unconfigured  unknown
usb0/1          unknown   empty       unconfigured  ok
usb0/2          unknown   empty       unconfigured  ok


secca38#tail /var/adm/messages

Nov  2 15:53:25 secca38 genunix: [ID 408114 kern.info] /pci@1f,700000/scsi@2/sd@0,1 (sd1)
online
```

Step 14 Use the **format** and **prtvtoc** commands to partition the new disk.

Disk layout:

```
Slice 0 /(root)2000MB
Slice 1 /var 5000MB
Slice 3 swap 4000MB
Slice 4 unassigned 24MB
Slice 5 /opt The rest of the disk space
Slice 6 unassigned 2000MB
```

Step 15 Create the database replica on the new disk.

```
<hostname>#metadb -a -f -c 3 /dev/dsk/cxt1d0s4
```

Step 16 Perform the following commands to create submirror metadevice.

```
<hostname>#metainit -f d0 1 1 /dev/dsk/cxt1d0s0
<hostname>#metainit -f d12 1 1 /dev/dsk/cxt1d0s6
<hostname>#metainit -f d9 1 1 /dev/dsk/cxt1d0s5
<hostname>#metainit -f d3 1 1 /dev/dsk/cxt1d0s1
<hostname>#metainit -f d6 1 1 /dev/dsk/cxt1d0s3
```

Step 17 Install the boot block on the new disk.

```
<hostname>#installboot /usr/platform/`uname -i`/lib/fs/ufs/bootblk /dev/rdsk/cxt1d0s0
```

Step 18 Sync Disk 1 (new disk) with Disk 0.

```
<hostname># metattach d2 d1
<hostname>#metattach d14 d13
<hostname>#metattach d11 d10
<hostname>#metattach d5 d4
<hostname>#metattach d8 d7
```

Note The disk sync process with take awhile depending on the disk size. To find out the percentage completion of this process, you can run the **metastat|grep %** command.

Step 19 Start all BTS 10200 platforms.

```
<hostname>#platform start -nocopy
```

APPENDIX A

Recoverable and Nonrecoverable Error Codes

Revised: July 22, 2009, OL-8000-32

This appendix lists normal, recoverable and nonrecoverable error codes for the Cisco BTS 10200 Softswitch. Table A-1 categorizes Media Gateway Control Protocol (MGCP) error codes into three categories: normal, recoverable, and non-recoverable. Table A-1 also provides some of the behaviors of the Cisco BTS 10200 Softswitch for different MGCP message error codes. Endpoint connection（EPCF) and audit connection（AUCX) messages are not sent by the Cisco BTS 10200 Softswitch to the gateway.

Table A-1 MGCP Normal, Recoverable, and Nonrecoverable Error Codes

MGCP Error Code	Description	AUEP	DLCX	CRCX	MDCX	RQNT
200	The requested transaction was executed normally.	N	N	N	N	N
250	The connection was deleted.	F	N	N	N	R
400	Transient error. If this code is received, the Cisco BTS 10200 Softswitch tries to recover by retransmitting the MGCP message with a different transaction identifier for a predefined number of times before declaring the endpoint faulty. The number of times is configurable at platform startup time, its default is 2.	R	R	R	R	R
401	Phone is already off-hook. If this code is received, the Cisco BTS 10200 Softswitch updates the endpoint resource state and continues with normal operation	F	F	R	N	N
402	Phone is already on-hook. If this code is received, the Cisco BTS 10200 Softswitch updates the endpoint resource state and continues with normal operation.	F	F	R	N	N
403	Endpoint does not have sufficient resources at this time. If this code is received, the Cisco BTS 10200 Softswitch automatically recovers by auditing the endpoint, deleting any available connections and then idling the endpoint.	R	F	N	N	R
404	Insufficient bandwidth at this time. If this code is received, the Cisco BTS 10200 Softswitch automatically recovers by auditing the endpoint, deleting any available connections and then idling the endpoint.	F	F	N	N	R
405	The transaction could not be executed, because the endpoint is “restarting.”	R	F	N	N	R

Table A-1 MGCP Normal, Recoverable, and Nonrecoverable Error Codes (continued)

MGCP Error Code	Description	AUEP	DLCX	CRCX	MDCX	RQNT
406	Transaction time-out. The transaction did not complete in a reasonable period of time and has been aborted.	R	F	N	N	R
407	Transaction aborted. The transaction was aborted by some external action, e.g. a ModifyConnection command aborted by a DeleteConnection command	R	F	N	N	R
500	Endpoint is unknown. If this code is received during idling of an endpoint, the Cisco BTS 10200 Softswitch marks the endpoint as faulty and perform automatic recovery.	F	F	F	N	F
501	Endpoint is not ready. If this code is received, the Cisco BTS 10200 Softswitch automatically recovers by auditing the endpoint, deleting any available connections and then idling the endpoint.	R	F	N	N	R
502	The transaction could not be executed, because the endpoint does not have sufficient resources (permanent condition)	R	F	N	N	R
503	“All of” wildcard too complicated	F	F	N	N	R
509	Error in RemoteConnectionDescriptor	F	F	F	N	F
510	The transaction could not be executed, because some unspecified protocol error was detected. Automatic recovery from such an error will be very difficult, and hence this code SHOULD only be used as a last resort	R	F	N	N	R
511	The transaction could not be executed, because the command contained an unrecognized extension. This code SHOULD be used for unsupported critical parameter extensions (“X+”)	F	F	F	N	F
512	The transaction could not be executed, because the gateway is not equipped to detect one of the requested events	F	F	N	N	F
513	The transaction could not be executed, because the gateway is not equipped to generate one of the requested signals.	F	F	N	N	F
514	The transaction could not be executed, because the gateway cannot send the specified announcement.	F	F	N	N	R
515	The transaction refers to an incorrect Connection-ID (may have been already deleted).	F	N	N	N	R
516	The transaction refers to an unknown Call-ID, or the Call-ID supplied is incorrect (e.g. Connection-ID not associated with this Call-ID).	F	N	N	N	R
517	Unsupported or invalid mode.	F	F	F	N	R
518	Unsupported or unknown package. It is RECOMMENDED to include a PackageList parameter with the list of supported packages in the response, especially if the response is generated by the Call Agent.	F	F	F	N	F

Table A-1 MGCP Normal, Recoverable, and Nonrecoverable Error Codes (continued)

MGCP Error Code	Description	AUEP	DLCX	CRCX	MDCX	RQNT
519	Endpoint does not have a digit map	F	F	N	N	R
520	The transaction could not be executed, because the endpoint is "restarting." In most cases this would be a transient error, in which case, error code 405 SHOULD be used instead. The error code is only included here for backwards compatibility	R	F	N	N	R
521	Endpoint redirected to another Call Agent. The associated redirection behavior is only well-defined when this response is issued for a RestartInProgress command	F	F	N	N	R
522	No such event or signal. The request referred to an event or signal that is not defined in the relevant package (which could be the default package).	F	F	N	N	F
523	Unknown action or illegal combination of actions	R	F	N	N	R
524	Internal inconsistency in LocalConnectionOptions.	F	F	N	N	R
525	Unknown extension in LocalConnectionOptions. This code SHOULD be used for unsupported mandatory vendor extensions ("x+").	F	F	F	N	R
526	Insufficient bandwidth. In cases where this is a transient error, error code 404 SHOULD be used instead.	F	F	N	N	R
527	Missing RemoteConnectionDescriptor.	F	F	F	N	R
528	Incompatible protocol version	F	F	F	N	F
529	Internal hardware failure	F	F	F	N	F
530	Channel-associated signaling (CAS) protocol error	R	F	N	N	R
531	Failure of a grouping of trunks (e.g. facility failure)	F	F	N	N	R
532	Unsupported value(s) in LocalConnectionOptions.	F	F	F	N	R
533	Response too large.	F	F	N	N	R
534	Codec negotiation failure.	F	F	N	N	R
535	Packetization period not supported.	F	F	N	N	R
536	Unknown or unsupported RestartMethod	F	F	N	N	R
537	Unknown or unsupported digit map extension	F	F	N	N	F
538	Event/signal parameter error (e.g. missing, erroneous, unsupported, unknown, etc.).	F	F	N	N	F
539	Invalid or unsupported command parameter. This code SHOULD only be used when the parameter is neither a package or vendor extension parameter	F	F	N	N	R
540	Per endpoint connection limit exceeded.	F	F	N	N	R
800		F	F	N	F	F
801		F	F	N	F	F
802		F	F	N	F	F

Table A-1 MGCP Normal, Recoverable, and Nonrecoverable Error Codes (continued)

MGCP Error Code	Description	AUEP	DLCX	CRCX	MDCX	RQNT
803		F	F	N	F	F
Unknown like 900		F	F	F	F	F
Invalid or absent transaction identifier		RX	RX	RX	RX	RX

Note AUEP—audit endpoint, DLCX—delete connection, CRCX—create connection, MDCX—modify connection, RQNT—notification request

Note Normal (N)—other than 200 error code, the Cisco BTS 10200 Softswitch clears the call. recoverable (R)—: the Cisco BTS 10200 Softswitch clears the call and starts finite recovery. non-recoverable (NR) or faulty (F)— the Cisco BTS 10200 Softswitch clears the call.

Note For 400 error codes, the Cisco BTS 10200 Softswitch re-transacts (RT) the corresponding MGCP message. The Cisco BTS 10200 Softswitch also retransmits (RX) the MGCP message with the same transaction.

APPENDIX **B**

System Usage of MGW Keepalive Parameters, Release 4.5.x

Revised: July 22, 2009, OL-8000-32

This appendix explains how the Cisco BTS 10200 Softswitch determines the connectivity status between itself and a media gateway (MGW). The BTS 10200 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-max-keepalive-interval (default = 600 seconds)
  - mgcp-t-tran (default = 400 milliseconds)
- In the call-agent table:
  - mgw-monitoring-enabled (default=Y)
- In the ca-config table:
  - mgcp-t-max (default = 20 seconds)
  - mgcp-rto-max (default = 4 seconds)

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 BTS 10200 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 BTS 10200 and the MGW. If there is a loss of connectivity, the BTS 10200 retries the series of AUEP transmissions up to a specified number of retries (defined by **mgcp-keepalive-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 BTS 10200 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 BTS 10200, see the MGW Status Command in the *BTS 10200 Operations and Maintenance Guide*.

The system uses the parameters **mgcp-max1-retries** and **mgcp-max2-retries** to limit the number of retransmissions of the same AUEP. 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 based on the description in RFC 3435, Section 4.3, and 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 following parameters are also related to MGW connection status, but are not discussed in detail in this appendix. For additional details, see the *BTS 10200 Command Line Reference Guide*.

- Long transaction (applicable to NCS endpoints)—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 Transmission Waiting Period (mgcp-t-tran)

The initial transmission waiting period (the period that the system waits after sending an initial AUEP transmission before repeating it) is equal to *the greater of* the following:

- The 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.

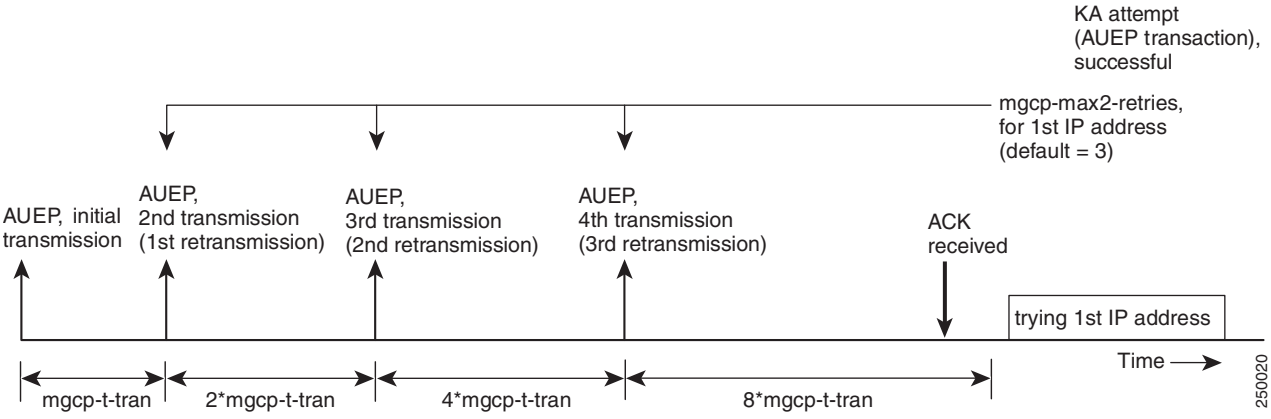
In a typical network, the average response time is much less than 400 milliseconds. Therefore, in this section, the drawings show the initial waiting period as **mgcp-t-tran**.

Note The drawings in this section are not to scale.

Scenarios with AUEP Message Retransmissions and ACK Received

Figure B-1 is applicable when one 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 retransmissions.

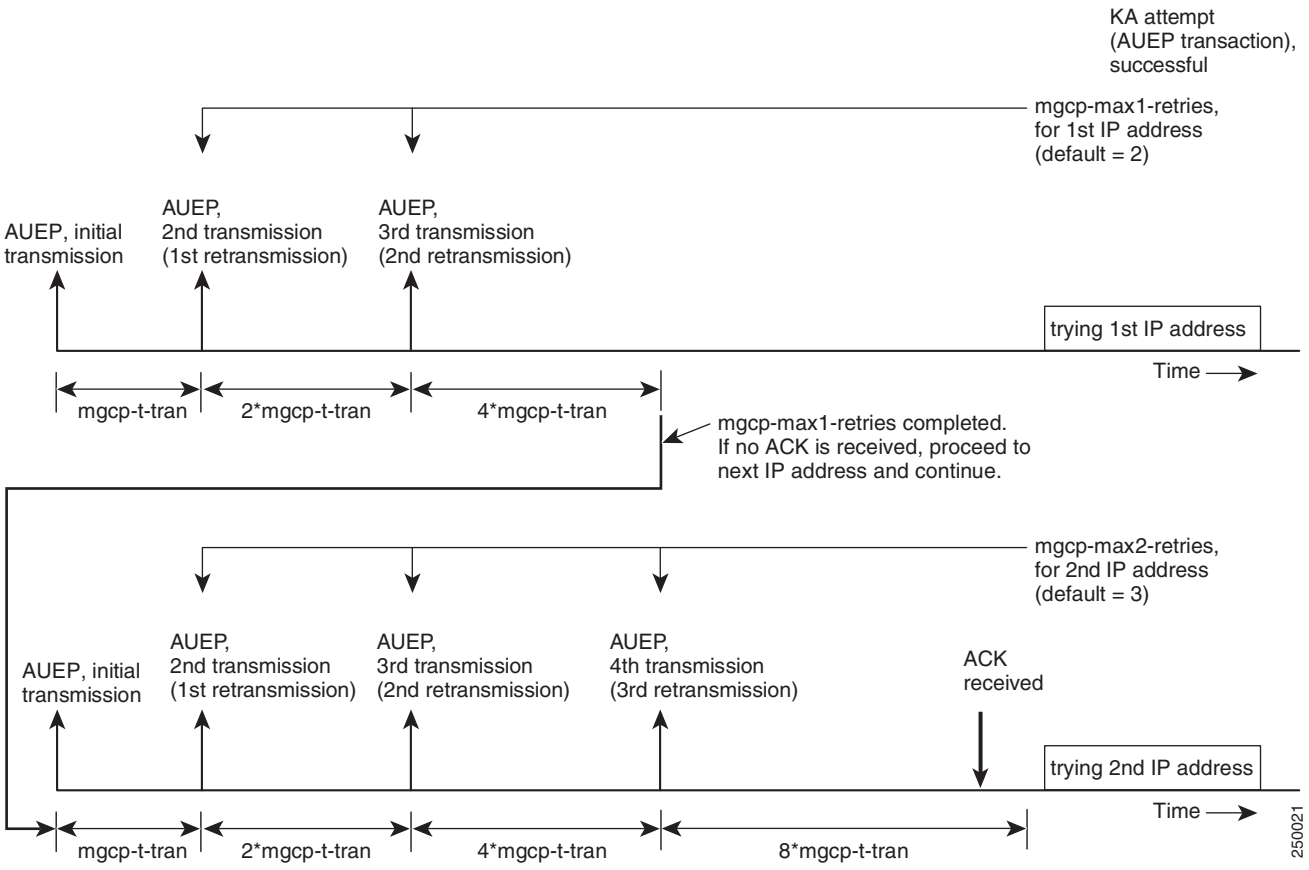
Figure B-1 One IP Address in DNS, ACK Received after Retransmissions



Note See the additional information about **mgcp-t-tran** in the "Initial Transmission Waiting Period (mgcp-t-tran)" section on page B-4.

Figure B-2 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 retransmissions.

Figure B-2 Two IP Addresses in DNS, ACK Received after Retransmissions



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.)

Scenarios with AUEP Message Retransmissions and No ACK

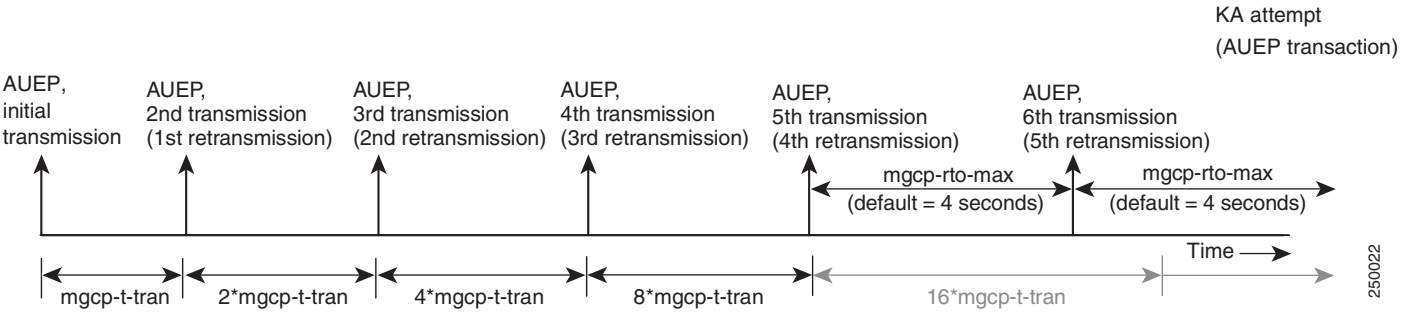
This section explains how the system handles MGCP message retransmissions and takes action when no ACK is received from the MGW.

MGCP-RTO-MAX

Figure B-3 shows how the system repeats the same AUEP message if an ACK is not received. The period between subsequent retransmissions increases by a factor of two, but is limited to a maximum of **mgcp-rto-max**.

Tip Terminology—Note that the first transmission is called the initial transmission. The second transmission of the same AUEP message is called the first retransmission (or the first retransmission).

Figure B-3 Example of Retransmission Timing (Upper Limit = mgcp-rto-max)



Note See the additional information about **mgcp-t-tran** in the "Initial Transmission Waiting Period (mgcp-t-tran)" section on page B-4.

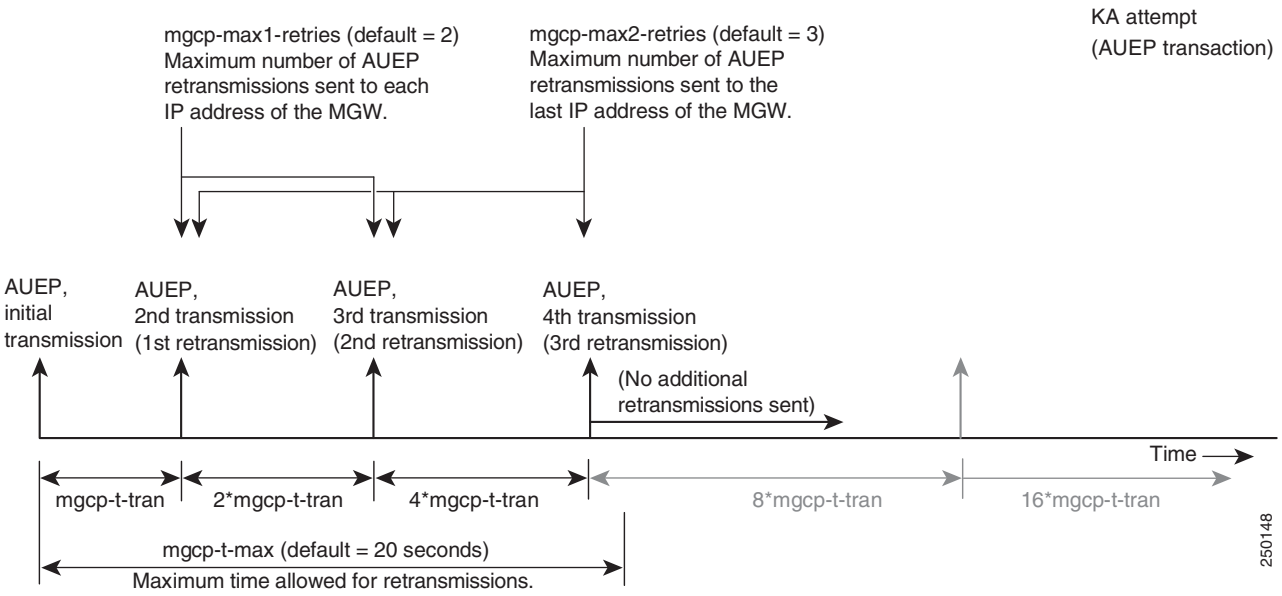
MGCP-MAX2-RETRIES and MGCP-T-MAX

The BTS 10200 limits retransmissions of the AUEP message to **mgcp-max2-retries** or a total duration of **mgcp-t-max** (default = 20 seconds), whichever occurs first. If the system has not received an ACK at this point, it takes the following actions:

- It stops all retransmissions and abandons the transaction.
- If keepalive functionality is *enabled* on the system (**mgw-monitoring-enabled=Y** and **keepalive-method=AUEP** as described in the "Provisionable Parameters" section on page B-1), the system expedites the KA process (as described in the "Keepalive Process" section on page B-7) 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. The operational status of each of the terminations is marked as TERM_UNREACH.
- If keepalive functionality is *disabled* on the system, the system marks the operational status of each of the terminations as UNKNOWN.

Figure B-4 shows how the system handles AUEP retransmissions and takes action if no ACK is received. In this example, mgcp-max2-keepalive attempts are completed before the expiration of mgcp-t-max. In general, the system stops retransmissions when mgcp-max2-keepalive attempts are completed or at the expiration of mgcp-t-max, whichever occurs first.

Figure B-4 Timeout Limitations When No ACK Is Received



Keepalive Process

This section describes the keepalive (KA) process. The BTS 10200 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=tgw**).

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:

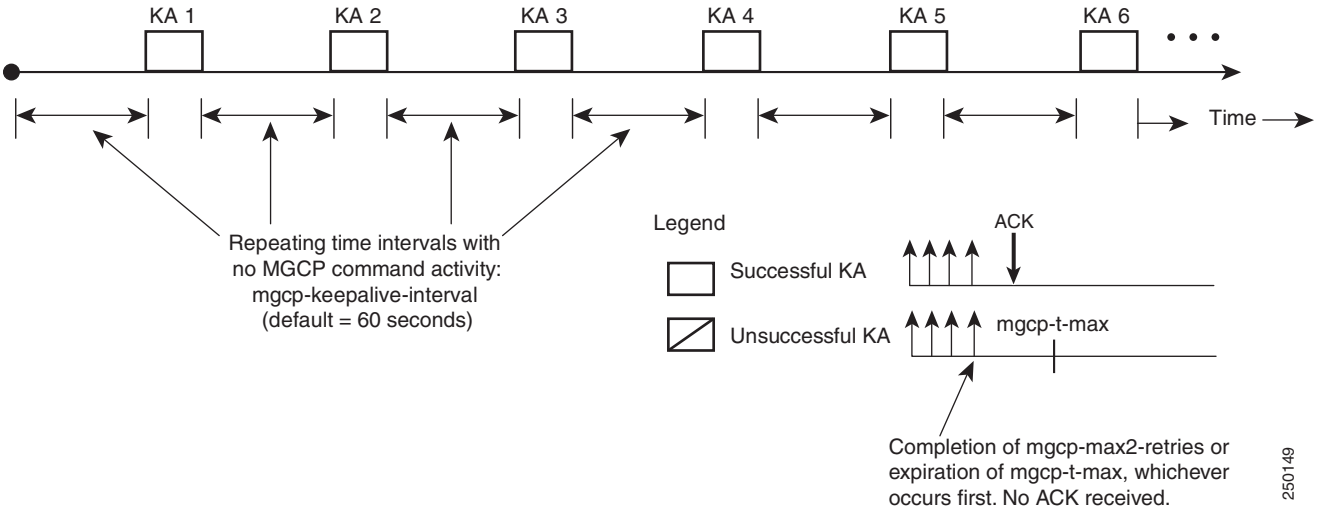
- Basic Scenario
- MGCP Message Sent and Is Unsuccessful
- MGCP Message Sent and Is Successful

Basic Scenario

The basic scenario is shown in Figure B-5. 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 BTS 10200 and the MGW for a time interval equal to the provisioned value of **mgcp-keepalive-interval** (default 60 seconds) in the **mgw-profile** table.

Note The legend in this drawing explains how successful and unsuccessful keepalive attempts are illustrated throughout this document.

Figure B-5 KA Attempts—MGW Reachable with Stable Calls



Note For detailed examples of successful KA attempts, see Figure B-1 and Figure B-2.

The system takes the following actions in the scenario shown in Figure B-5:

- 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.)

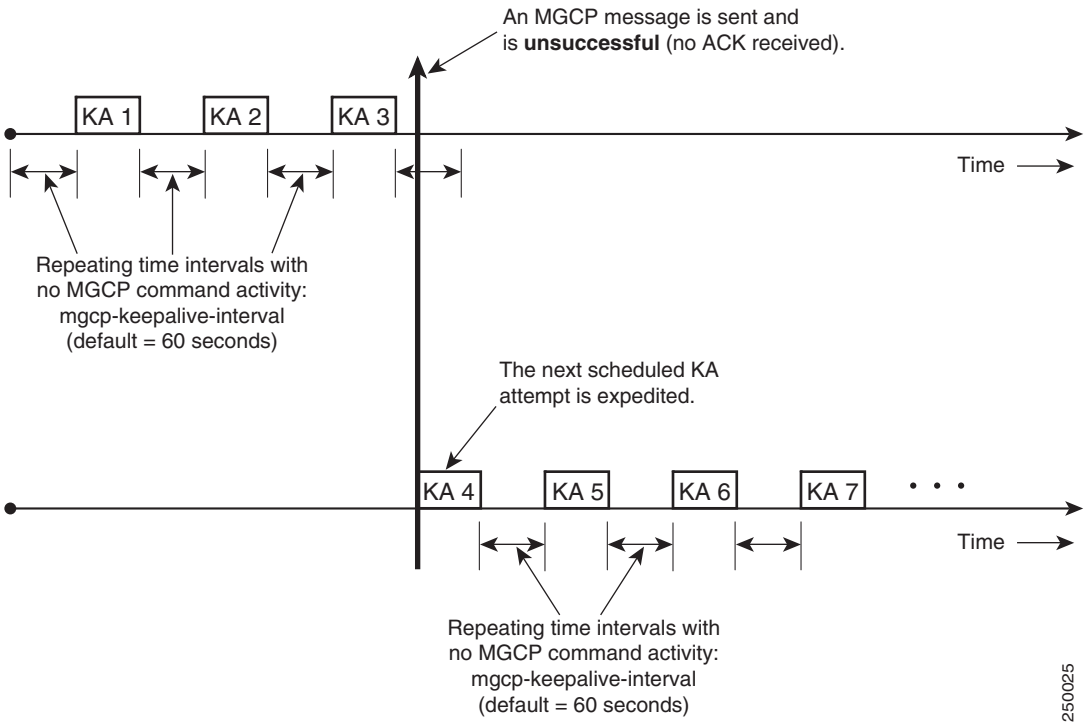
Note For TGWs and RGWs with more than 16 endpoints—If a KA attempt is successful, the system continues to implement Scenario 1 regardless of whether there are stable calls or not.

- 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 BTS 10200 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 B-6.

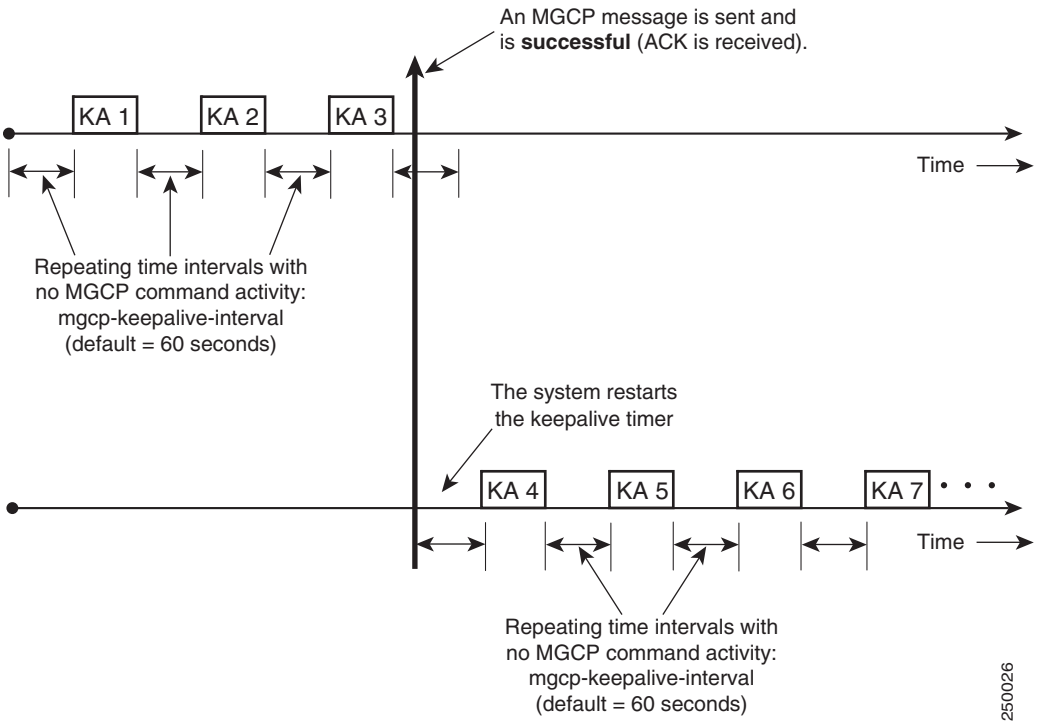
Figure B-6 MGW Reachable with Stable Calls, and MGCP Message Unsuccessful



MGCP Message Sent and Is Successful

If the BTS 10200 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 B-7.

Figure B-7 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 BTS 10200 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.)

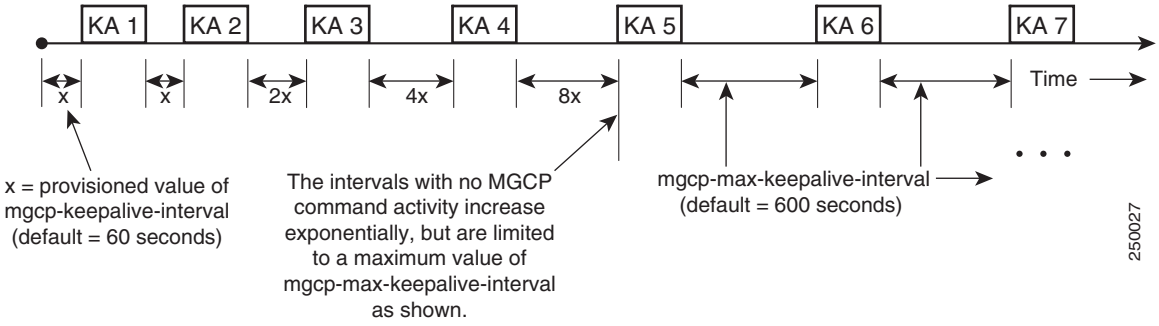
Three variations of this scenario are described in this section:

- Basic Scenario
- MGCP Message Sent and Is Unsuccessful
- MGCP Message Sent and Is Successful

Basic Scenario

The basic scenario is shown in Figure B-8. 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 BTS 10200 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 B-8 KA Attempts—MGW Reachable with No Stable Calls



Note For detailed examples of successful KA attempts, see Figure B-1 and Figure B-2.

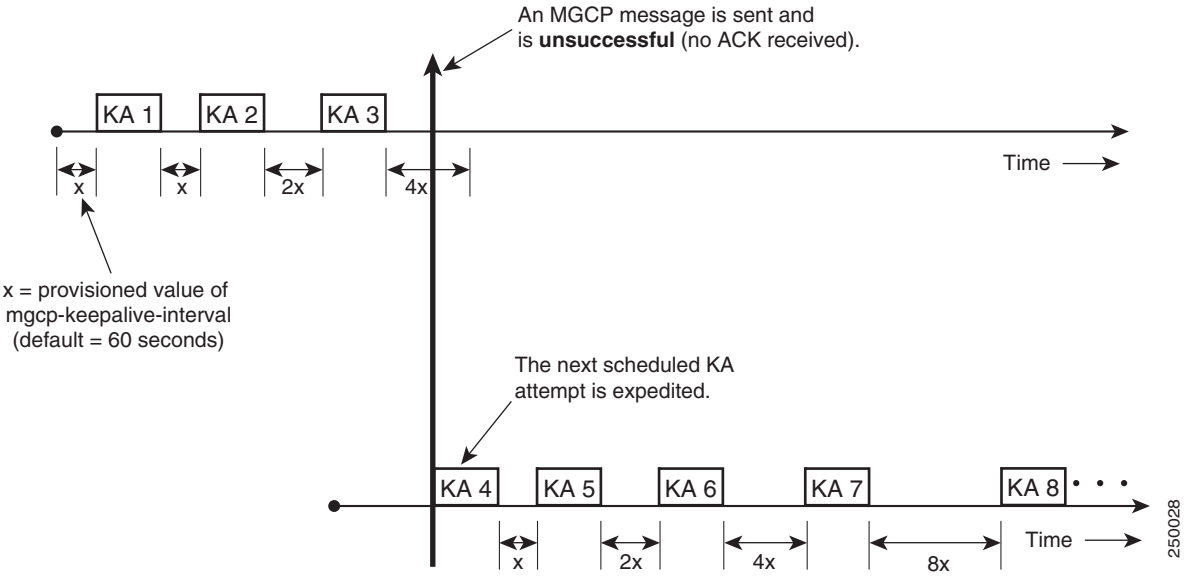
The system takes the following actions in the scenario shown in Figure B-8:

- 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 BTS 10200 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 B-9.

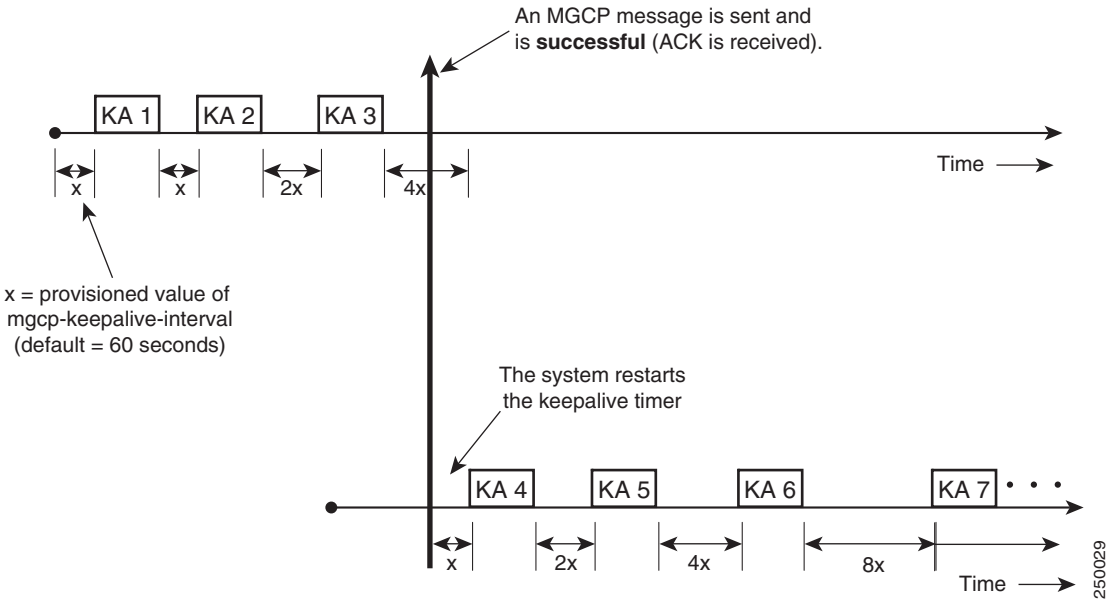
Figure B-9 MGW Reachable with No Stable Calls, and MGCP Message Unsuccessful



MGCP Message Sent and Is Successful

If the BTS 10200 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 B-10.

Figure B-10 MGW Reachable with No Stable Calls, and MGCP Message Successful



Scenario 3—MGW Unreachable

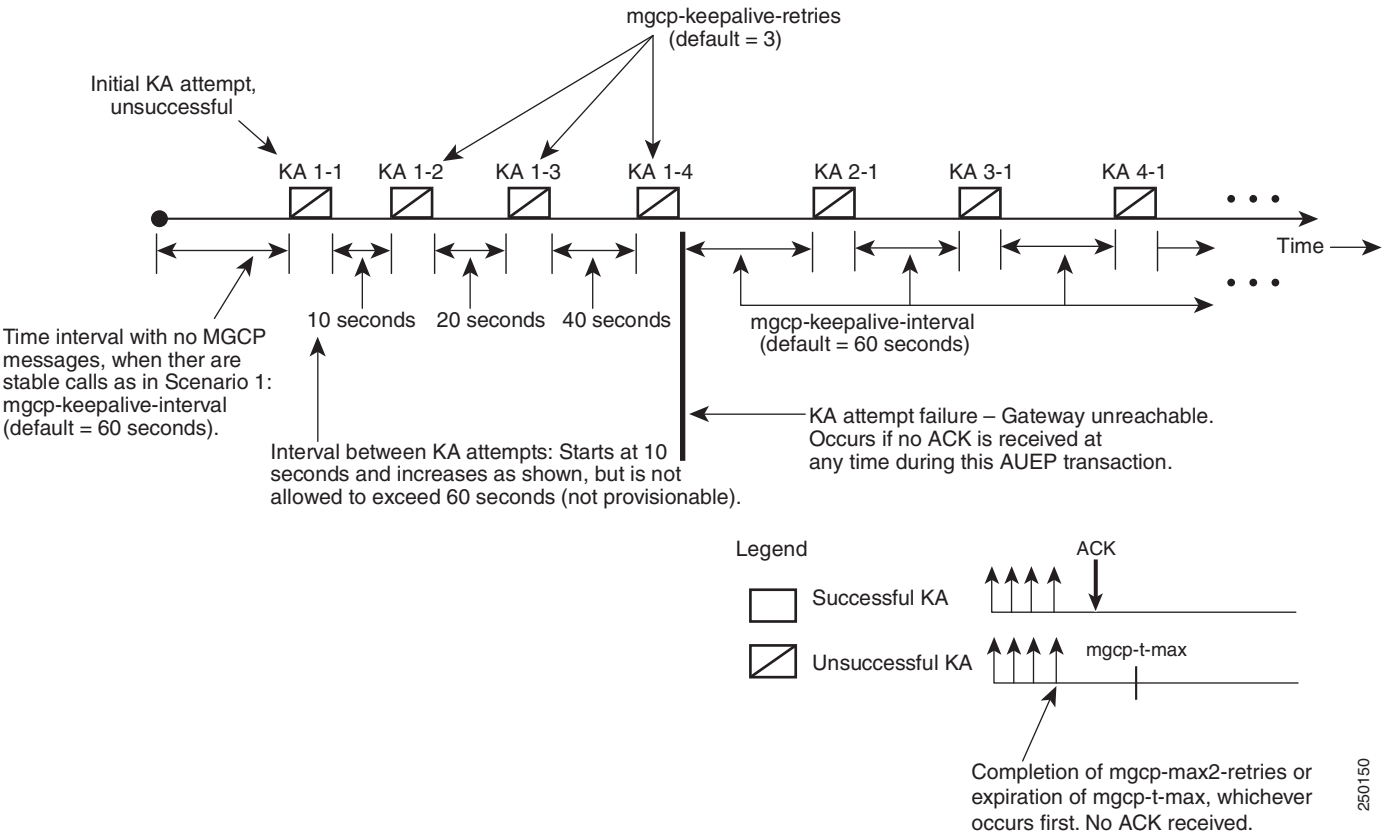
This scenario applies to residential gateways (RGWs) and trunking gateways (TGWs). The following conditions are described:

- KA Attempts Unsuccessful, MGW Unreachable, and Stable Call Is Present
- KA Attempts Unsuccessful, MGW Unreachable, and No Stable Calls Present
- MGW Unreachable, New Call Termination Attempt Occurs

KA Attempts Unsuccessful, MGW Unreachable, and Stable Call Is Present

If no ACK is received during any KA attempt, and no MGCP messages have been exchanged between the BTS 10200 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 B-11 for the case with stable call(s) present.

Figure B-11 KA Attempts Unsuccessful, MGW Unreachable, and Stable Call Is Present



Notes for Figure B-11

- The keepalive attempts labeled KA 1-2, KA 1-3, and KA 1-4 represent retries of the original keepalive attempt KA 1-1. The number of retries is provisioned as **mgcp-keepalive-retries**.
- The keepalive attempts labeled KA 2-1, KA 3-1, and further, represent new attempts spaced according to the provisioned value of **mgcp-keepalive-interval**.
- Each keepalive attempt, KA 1-1, KA 1-2, ... KA 2-1, KA 3-1, and further, has a unique MGCP transaction ID.

Note For detailed examples of successful KA attempts, see Figure B-1 and Figure B-2.

The system takes the following actions in the scenario shown in Figure B-11:

- If a KA attempt is 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 a KA attempt is 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: The system raises one or more alarms and continues this pattern of KA attempts (Scenario 3—MGW Unreachable). For any stable calls on this MGW, the system takes the action specified in the spare1-supp token in the mgw-profile table.

  Typical alarms for this condition include:

  – SIGNALING (36)—Trunk locally blocked (applicable to CAS, ISDN, and SS7 trunks).

  – SIGNALING (79)—Media Gateway unreachable.

  Typical informational events for this condition include:

  – SIGNALING (152)—Termination transient error received. This event is applicable when the keepalive functionality is enabled.

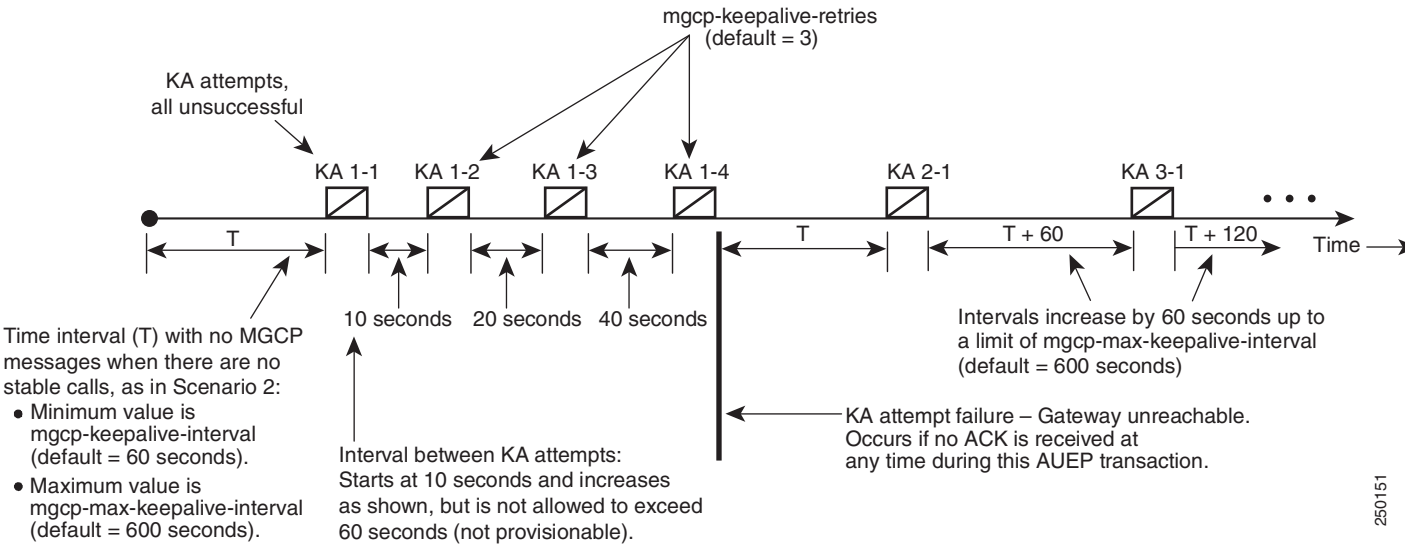
  – SIGNALING (76)—Timeout on remote instance. This event is applicable when the keepalive functionality is disabled.

- If all KA attempts are unsuccessful through **mgcp-keepalive-retries**, the system declares the MGW unreachable.

KA Attempts Unsuccessful, MGW Unreachable, and No Stable Calls Present

This condition is similar to the condition described in "KA Attempts Unsuccessful, MGW Unreachable, and Stable Call Is Present" section on page B-13. However, the intervals that occur after the KA attempt failure are different. This condition, with no stable calls present, is shown in Figure B-12.

Figure B-12 KA Attempts Unsuccessful, MGW Unreachable, and No Stable Calls Present

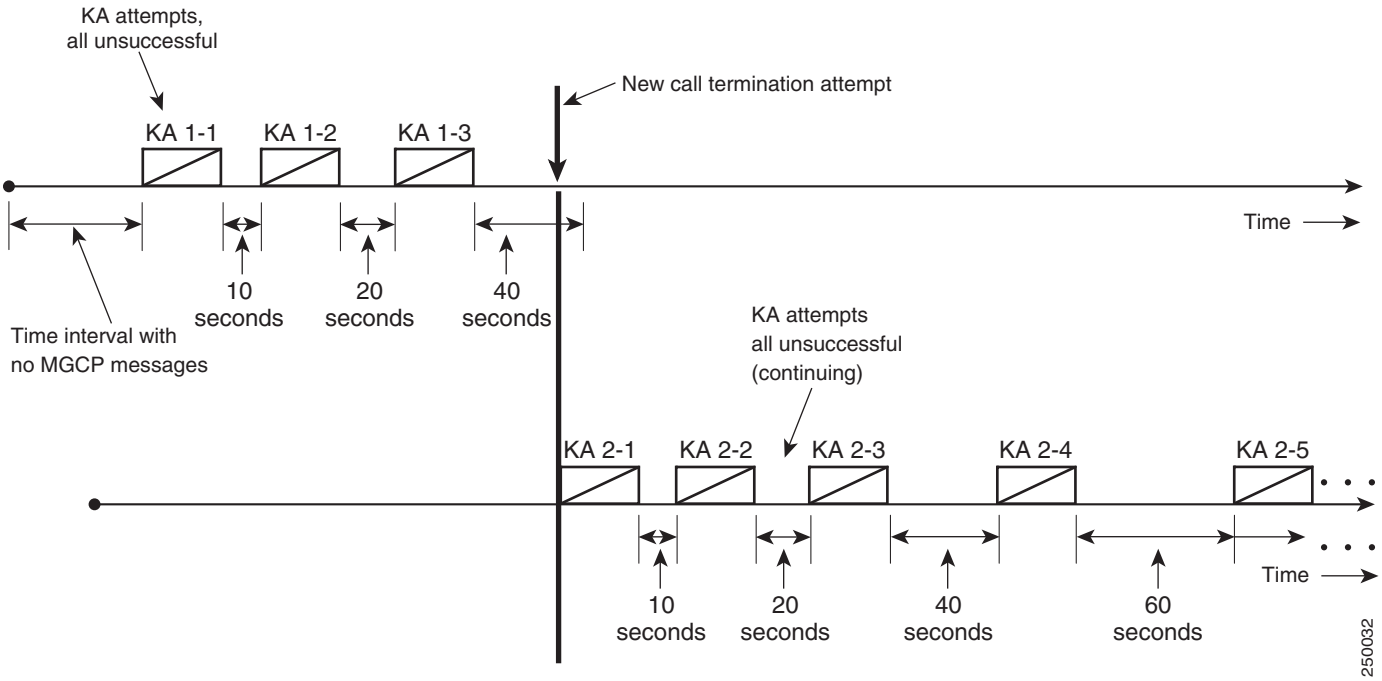


MGW Unreachable, New Call Termination Attempt Occurs

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 B-13.

Note In this case, the BTS 10200 fails the call immediately after receiving the call termination attempt, without sending any MGCP message to the MGW.

Figure B-13 MGW Unreachable, New Call Termination Attempt Occurs



GLOSSARY

Revised: July 22, 2009, OL-8000-32

A

AAA	authentication, authorization, and accounting
ACAR	automatic callback and automatic rollback
ACF	admission confirmation
ACG	automatic call gapping
ACK	acknowledge
ACL	access control list, automatic congestion level
ACTV	active
ADDR	address
ADM	administrative
AGGR	aggregation
AIN	Advanced Intelligent Network
ALT	alternate
ANC	announcements module
ANI	automatic number identification
ANSI	American National Standards Institute
AOR	address of record
API	application programming interface
ARQ	admission request
AS	application server
ASC	associate
ASP	application service provider
ATIS	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

CIC circuit identification code, carrier identification code

CLI command line interface

CLLI common language location identifier

CMJ circuit reservation rejected

CMTS cable modem termination system

CNAM calling name delivery

CODEC coder/decoder, compression/decompression

COPS Common Open Policy Service Protocol

CORBA Common Object Request Broker Architecture

COT customer-originated trace, continuity testing, central office termination

CPE customer premises equipment

CPU central processing unit

CQM circuit query message

CQR circuit query response

CRC cyclic redundancy check

CRCX create connection

CS capability set (for example, CS-2)

CST Central Standard Time

CTRL control

CTX Centrex

CVM circuit verification message

CVR circuit verification response

CVT circuit validation test

D

DB database

DBA database administrator

DBM database management

DF delivery function

DHCP Dynamic Host Configuration Protocol

DLCX delete connection

DLY delay

DN directory number

DNIS dialed number identification service

DNS domain name system

DOC document

DPC destination point code

DSCP differentiated service code point

DUPU destination user part unavailable

E

EA equal access

EGA event generator

EM event message

EMEA Europe, Middle East, and Asia

EMS Element Management System

EP endpoint

EPCF endpoint connection

ER easily recognizable

ESA enhanced subscriber authentication

ESF extended super frame

F

FAS facility associated signaling

FPGA field programmable gate array

FQDN fully qualified domain name

FS	Feature Server
FSAIN	Feature Server for AIN services
FSPTC	Feature Server for POTS, Tandem, and Centrex services
FTP	File Transfer Protocol
FXS	Foreign Exchange Station

G

GAP	generic address parameter
GB	gigabits
GCF	gatekeeper confirmation
GK	gatekeeper
GMT	Greenwich Mean Time
GRA	group reset acknowledge
GRJ	gatekeeper reject
GRP	group
GRQ	gatekeeper request
GRS	group reset
GTD	generic transport descriptor
GTT	global text telephony
GW	gateway

H

H323	H.323 Protocol
H323GW	H323 gateway
H3A	H.323 signaling adapter
HB	heartbeat

I

IAD	integrated access device
IAM	initial address message
ICMP	Internet Control Message Protocol
ID	identification
IDX	index
IE	information element
IETF	Internet Engineering Task Force
IN	intelligent network
INF	information
INFO	information
INIT	initialize
INR	information request
INS	in service
IOS	Integrated Operating System
IP	Internet Protocol
IPC	inter-process communication
IPM	Internet Protocol Manager
IPSEC	Internet Protocol security
ISDN	Integrated Services Digital Network
ISP	Internet service provider
ISUP	ISDN user part
ITP	IP transfer point
IVR	interactive voice response
IXC	interexchange carrier

J

JMS	Java message service

K

KAM keepalive module

KB kilobit

KMS Kerberized management server

L

LAF log archive facility

LATA local access and transport area

LBLK locally blocked

LIDB line information database

LNP local number portability

LPA loop prevention acknowledgement

LRN local routing number

LSA local serving area

M

M3UA MTP3 user adapter

MB megabit

MDCX modify connection

MDL message definition language

MGA media gateway adapter

MGCP Media Gateway Control Protocol

MGW media gateway

MIB Management Information Base

MIM M3UA Interface Module

MRMW multiple readers and multiple writers

ms millisecond

MTA media terminal adapter, Metropolitan Trading Area

MTP message transfer part

MTP1 message transfer part 1

MTP2 message transfer part 2

MTP3 message transfer part 3

MTU maximum transmission unit

N

NANP North American Numbering Plan

NAS network access server

NCS network-based call signaling

NFAS non-facility associated signaling

NFS network file server

NIIF Network Interconnection Interoperability Forum

NMS network management system

NNN numeric number nomenclature

NOA nature of address

NPA Numbering Plan Area

NPAC Number Portability Administration Center

NR non-recoverable

NTP Network Time Protocol

NU network unit

NUM number

NW network

O

OAMP operations, administration, maintenance and provisioning

OLI originating line information

OMNI Ulticom SS7 stack

OMS OptiCall Messaging System

OPC originating point code

OPT Open Packet Telephony

ORA Oracle

OS operating system

OSS operations support system

P

PBX private branch exchange

PDM process debug manager

PDU protocol decode unit

PIC presubscribed interexchange carrier, point in call

PID process ID

PMG process manager

POP point of presence

POTS plain old telephone service

PRI primary rate interface

PSTN 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

RTP Real Time Transport Protocol

RUDP Reliable User Datagram Protocol

RX retransmit

S

S1 severity 1

S2 severity 2

S3 severity 3

S4 severity 4

S7A	SS7 adapter
S7M	SS7 module
SA	security association
SAI	signaling adapter interface
SAP	service access point
SCA	selective call acceptance, status control adapter
SCC	signaling connection control
SCCP	signaling connection control part
SCP	service control point, signal control point
SCTP	Stream Control Transmission Protocol
SDN	software defined network
SFTP	Secure File Transfer Protocol
SG	signaling gateway
SGP	signaling gateway process
SHR	System Health Report (system-health)
SIA	SIP adapter
SID	system identification number
SIP	Session Initiation Protocol
SLC	signaling link code
SLHR	Service Logic Host Route
SM	system manager
SMG	system manager program
SMS	service management system
SNMP	Simple Network Management Protocol
SP	service provider
SQL	Structured Query Language
SRV	service
SS7	Signaling System 7
SSH	secure shell

SSN subsystem number

SSP signal switching point

STP signal transfer point

SUA SCCP user adapter

SUB subscriber

T

T1 trunk level 1

T3 trunk level 3

T5 timer 5

T13 timer 13

T15 timer 15

T17 timer 17

T19 timer 19

T21 timer 21

T23 timer 23

T28 timer 28

T_{CCR} timer continuity check request

TAC Technical Assistance Center

TCAP Transaction Capabilities Application Part

TCP Transmission Control Protocol

TDM telecommunications data link monitor

TEI terminal endpoint identifier

TFC transfer controlled

TG trunk group, trunking gateway

TGID trunk group ID

TGN-ID trunk group ID

TMM Traffic and Measurements module

TOS type of service

TPM terminating point master

TRNS transient

TSA TCAP signaling adapter

TSAP transport service access point

TT translation type

TVT Translation Verification Tool

U

UBL unblocking message

UDP User Datagram Protocol

UEQP unequipped

ULP Upper Layer Protocol

URI uniform resource identifier

URL universal resource locator

US United States

USA 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