Cisco BTS 10200 Softswitch Troubleshooting Guide, Release 6.0.3

Revised: August 10, 2011

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-25016-01

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

Cisco BTS 10200 Softswitch Troubleshooting Guide, Release 6.0.3

CONTENTS

Preface

Revised: August 10, 2011, OL-25016-01

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

Organization

This Troubleshooting Guide contains the following chapters:

- Chapter 1, "Troubleshooting Overview"—Provides an overview of troubleshooting the Cisco BTS 10200.
- 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.
- Chapter 14, “General Troubleshooting”—Provides the general troubleshooting information needed to conduct troubleshooting on the Cisco BTS 10200.
- 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 system.
- Appendix A, “Recoverable and Nonrecoverable Error Codes”—Lists normal, recoverable and nonrecoverable error codes for the Cisco BTS 10200.
- Appendix B, “System Usage of MGW Keepalive Parameters, Release 6.0”—Explains how the Cisco BTS 10200 determines the connectivity status between itself and a media gateway (MGW).
- Appendix C, “Overload Control”—Overload is a switch condition that exists when system resources cannot handle system tasks. Increases in call traffic or messages indirectly related to call traffic usually cause overload.

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.

Document Change History

The following table lists the revision history for the *Cisco BTS 10200 Softswitch Troubleshooting Guide, Release 6.0.3*.

Version Number	Issue Date	Status	Reason for Change
OL-25016-01	10 Aug 2011	Initial	Initial document for Release 6.0.3.

CHAPTER 1

Troubleshooting Overview

Revised: August 10, 2011, OL-25016-01

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 telecommunication companies 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.

Note Refer to the "Obtaining Documentation and Submitting a Service Request" section on page l for detailed instructions on contacting Cisco Technical Assistance Center (TAC) and opening a service request.

Interoperability

The Cisco BTS 10200 inter-works with a wide range of network elements (NEs), but there are certain limitations. We recommend 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, multimedia terminal adapters (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 Release 6.0 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.

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. You should always use 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, 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 managing the alarm and error messages is provided in the "Managing Events and Alarms" section on page 1-8.

General Problem-Solving Model

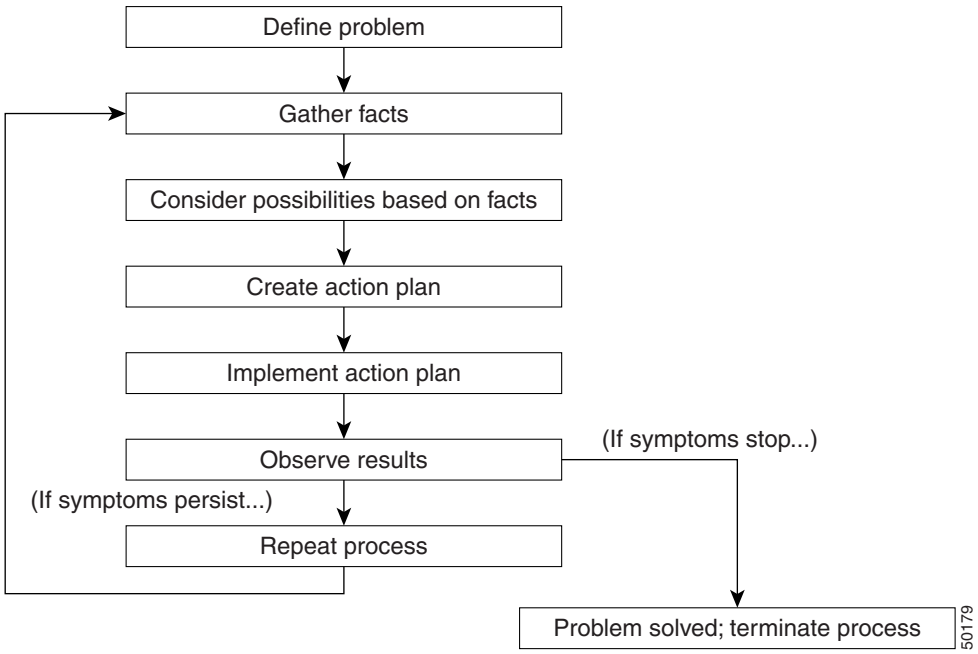
When you are troubleshooting in a telephony environment, a systematic approach always works best. An unsystematic approach to troubleshooting can result in a "quick fix" but it is usually a waste of valuable time and resources and often makes the situation worse.

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 on 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, and 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 allows 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 those 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. 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?

- Do you know current software and patch version?

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 and 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, minimizes 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 the 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
- Current software version and patch level
- Note any recent configuration, software, or topology changes

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

Caution These are not upgrade procedures. Performing the steps in these restoration 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.

Caution If both an active and a standby application file become corrupted, contact Cisco TAC immediately.

Figure 1-2 Problem Identification

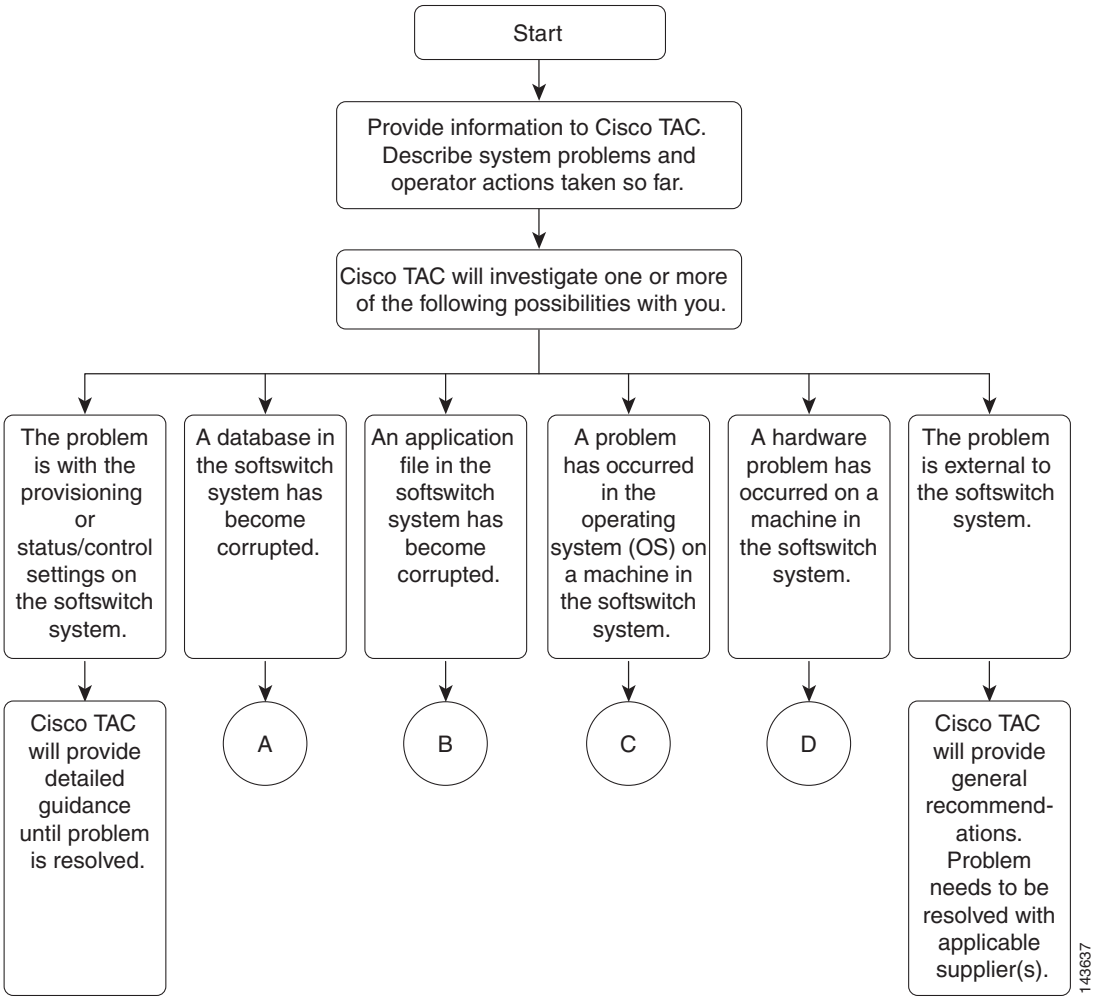
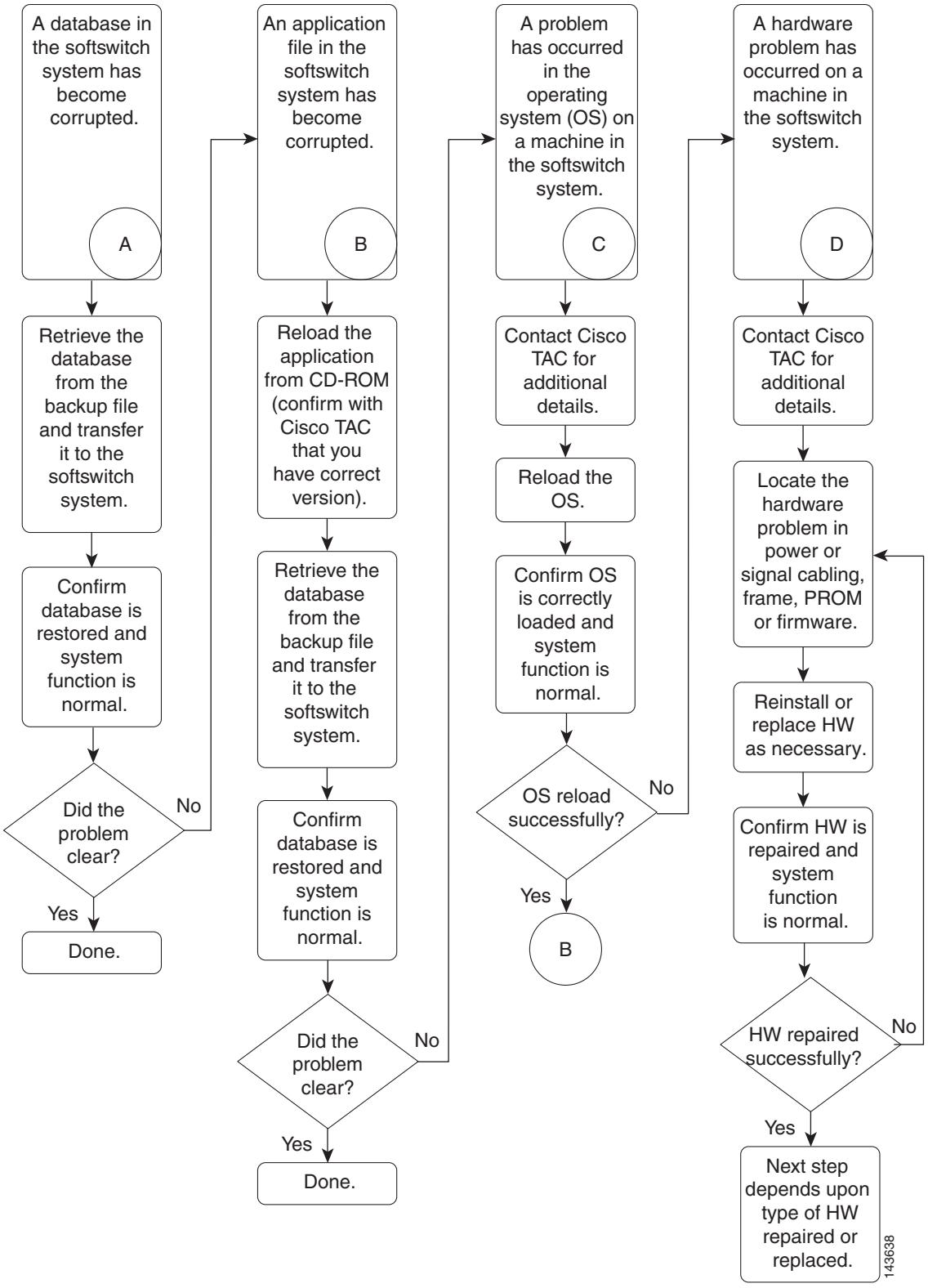


Figure 1-3 Resolving Database, Application, Operating System (OS) and Hardware Problems



Managing Events and Alarms

The Cisco BTS 10200 generates messages or events to notify you of network conditions. Events with severity levels of critical, major, or 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 software writes event and alarm messages to log files that are set up during system initialization. This section 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:

Note Refer to the Cisco BTS 10200 Softswitch CLI Database 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. To be notified of alarms as they occur, subscribe to the event and alarm reports. To display a list of current events or alarms, use the **show alarm** command.

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>;
order=ID;
```

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 following example illustrates that certain fields of the alarm can be displayed using the display option:

```
CLI> show alarm; order=id; display=severity,number; limit=5

Severity=MAJOR
NUMBER=114

Severity=MAJOR
NUMBER=109

Severity=MAJOR
NUMBER=6

Severity=MAJOR
NUMBER=114

Severity=MAJOR
NUMBER=109

Reply: Success: Entries 1-5 of 138 returned.
```

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
- **component-id**—The identification (ID) of the component reporting the alarm(s) (1 to 32 ASCII characters).
- **origin**—The internal designation of the process generating the alarm(s) (1 to 64 American Standard Code for Information Interchange (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)
- **order**—Enables the listing the events and alarms in chronological order.

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
- **component-id**—The identification (ID) of the component reporting the alarm(s) (1 to 32 ASCII characters).
- **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.

- **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, that is, 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 applies only to Cisco BTS 10200 systems that have 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 is 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.cisco.test
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 number. Event or alarm numbers are preset in the Cisco BTS 10200. They are not provisionable and cannot be changed.
Event or Alarm Type	Type is the designated category of the report: audit, billing, call processing (CALLP), configuration, database, maintenance, operations support system (OSS), security, signaling, statisitics, or system.
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 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 fail overs

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>; order=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>; order=id;
```

Both the **show even-log** command and the **show alarm-log** command can use the display option as shown in the following examples.

Example 1:

```
CLI> show alarm-log; order=id; display=severity, number; limit=5

Severity=MINOR
NUMBER=36

Severity=MINOR
NUMBER=36

Severity=MINOR
NUMBER=36

Severity=MINOR
NUMBER=36

Severity=MINOR
NUMBER=36

Reply: Success: Entries 1-5 of 30000 returned.
```

Example 2:

```
CLI> show event-log; order=id; display=severity, number; limit=5

Severity=WARNING
NUMBER=27

Severity=WARNING
NUMBER=27

Severity=INFO
NUMBER=58

Severity=INFO
NUMBER=58

Severity=WARNING
NUMBER=32

Reply: Success: Entries 1-5 of 30117 returned.
```

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, up to 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, that is, if you do a **show alarm-log limit=1**; and reply says 1 of 32008, then EGA would delete the 2008 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 and 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 We recommend 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=Not applicable
DW7NAME=Not applicable
DW8NAME=Not applicable
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, that is, 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 1-17).

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 1-17).

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 1-17).

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 fail overs.

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 1-19.

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 correcting the reason for the alarm will cause the alarm to reappear.

Events and Alarms Descriptions and Corrective Actions

This section provides an overview of the events and alarms that are generated by the Cisco BTS 10200 software.

Format of Events and Alarms

System messages, informational events, and alarms reported by the Cisco BTS 10200 are discussed in this section. Headings in left column (as shown in the following 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.

There are eleven types of Cisco BTS 10200 events and alarms:

- 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 (CALLP). Refer to Chapter 4, "Call Processing Troubleshooting."
- Configuration—Events or alarms 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 operations support system (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 fail overs (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 fail overs. 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 (INFO) 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.

Under normal operating conditions, no alarms should occur. However, any alarms that do occur should be investigated immediately. It is normal for events of informational 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 by CLI or other 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, anything beyond that is discarded if it is received during the 30 minute interval. After the 30 minute interval (on the hour and half-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) is transmitted and every event in between is discarded. The only exception is when the throttle set to 0, which means there is no throttle and all events are sent (up to the maximum threshold).

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

Data Reported

Depending on the specific event or alarm being reported, additional data fields (parameters) can 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, the actions are numbered and described in the order in which they should be performed.

New Events and Alarms (Release 5.0 to Release 6.0)

Table 1-2 lists the new events and alarms that were incorporated into the Cisco BTS 10200 system as part of the update from Release 5.0 to Release 6.0.

Table 1-2 New Events and Alarms (Release 5.0 to Release 6.0)

Type and Number	Description
Billing (60)	Bad File Detected During Startup
Call Processing (46)	Limit of Calls Allowed for the Pool Has Been Reached
Call Processing (47)	System Limit of Calls Allowed for Pools Has Been Reached
Maintenance (124)	Periodic Shared Memory Sync Started
Maintenance (125)	Periodic Shared Memory Sync Completed
Maintenance (126)	Periodic Shared Memory Sync Failure
OSS (17)	Session Has Been Removed
OSS (18)	Invalid Session Request
OSS (19)	Interface is Active and Operational
OSS (20)	Interface is Not Started or is Not Operational
OSS (21)	Resource Reset
OSS (22)	One Peer in the Realm is Out of Contact
OSS (23)	All Peers in the Realm are Out of Contact
OSS (24)	User Log In Sessions have Reached the User Session Limit
OSS (25)	Event Keep Alive Checked
Security (7)	Authentication Based On Credentials Failed
Signaling (178)	Possible Overlap Dialing Misconfiguration
Signaling (179)	Trunk Group Registration Expired

Modified Events and Alarms (Release 5.0 to Release 6.0)

Table 1-3 lists the Cisco BTS 10200 events and alarms that were modified as part of the upgrade from Release 5.0 to Release 6.0.

Table 1-3 Modified Events and Alarms (Release 5.0 to Release 6.0)

Type and Number	Description
Billing (60)	Bad File Detected During Startup
Maintenance (77)	Mate Time Differs Beyond Tolerance
Signaling (57)	Continuity Recheck Failed
Signaling (70)	Integrated Services Digital Network Unable to Restore D-channel Due to Failed Communication
Signaling (105)	Aggregation Gate Set Failed (AGGR Gate Set Failed)
Signaling (124)	Remote Subsystem is Out Of Service

Deleted Events and Alarms (Release 5.0 to Release 6.0)

Table 1-3 lists the Cisco BTS 10200 events and alarms that were deleted as part of the upgrade from Release 5.0 to Release 6.0.

Table 1-4 Deleted Events and Alarms (Release 5.0 to Release 6.0)

Type and Number	Description
Maintenance (105)	Unprovisioned Aggregration Device Detected
Maintenance (106)	Aggregration Device Address Resolution Failure

CHAPTER 2

Audit Troubleshooting

Revised: August 10, 2011, OL-25016-01

Introduction

This chapter provides the information needed for monitoring and troubleshooting 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 for monitoring and correcting the audit events
- Troubleshooting Audit Alarms—Provides the information needed for troubleshooting and correcting the audit alarms

Audit Events and Alarms

This section provides a brief overview of the audit events and alarms for the Cisco BTS 10200 Softswitch; the event and alarms are arranged in numerical order. Table 2-1 lists all of the audit events and alarms by severity.

Note Refer to the "Obtaining Documentation and Submitting a Service Request" section on page l for detailed instructions on contacting Cisco Technical Assistance Center (TAC) and opening a service request.

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	Information	Not Used
Audit (5)	Audit (6)	Audit (7)	Audit (3)	Audit (1)	Audit (9)
Audit (11)	Audit (12)	Audit (13)	Audit (4)	Audit (2)	
Audit (15)	Audit (17)	Audit (16)	Audit (8)	Audit (10)	
Audit (18)	Audit (20)		Audit (14)	Audit (21)	
	Audit (25)		Audit (19)	Audit (22)	
			Audit (23)		
			Audit (24)		

Audit (1)

Table 2-2 lists the details of the Audit (1) informational event. For additional information, refer to the "Test Report—Audit (1)" section on page 2-16.

Table 2-2 Audit (1) Details

Description	Test Report
Severity	Information
Threshold	100
Throttle	0
Primary Cause	This event is used for testing the new audit category.
Primary Action	No action is necessary.

Audit (2)

Table 2-3 lists the details of the Audit (2) informational event. For additional information, refer to the "Start or Stop of Signaling System 7—Circuit Identification Code Audit—Audit (2)" section on page 2-16.

Table 2-3 Audit (2) Details

Description	Start or Stop of Signaling System 7-Circuit Identification Code Audit (Start or Stop of SS7-CIC Audit)
Severity	Information
Threshold	100
Throttle	0
Datawords	Type of Audit—STRING [64]
Primary Cause	The Signaling System 7 (SS7) circuit identification code (CIC) audit has started or stopped.
Primary Action	No action required. This is normal operation.

Audit (3)

Table 2-4 lists the details of the Audit (3) warning event. 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 2-16.

Table 2-4 Audit (3) Details

Description	Signaling System 7 Circuit Identification Code Audit Terminated Before Successful Completion (SS7 CIC Audit Terminated Before Successful Completion)
Severity	Warning
Threshold	100
Throttle	0
Datawords	Type of Audit—STRING [64]
Primary Cause	A higher priority SS7 CIC audit interrupted and terminated a lower priority SS7 CIC audit.
Primary Action	Do not schedule an SS7 remote termination audit to occur while a periodic SS7 local termination audit is executing.

Audit (4)

Table 2-5 lists the details of the Audit (4) warning event. To monitor and correct the cause of the event, refer to the "Call Exceeds a Long-Duration Threshold—Audit (4)" section on page 2-16

Table 2-5 Audit (4) Details

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	A call exceeded the current system long-duration threshold.
Primary Action	If there is a reason to believe the call is no longer valid, release the associated trunk facility.

Audit (5)

Table 2-6 lists the details of the Audit (5) critical alarm. To troubleshoot and correct the cause of the alarm, refer to the "Critical Internal Audit Failure—Audit (5)" section on page 2-21.

Table 2-6 Audit (5) Details

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 the data field.
Primary Action	See the data field.

Audit (6)

Table 2-7 lists the details of the Audit (6) major alarm. To troubleshoot and correct the cause of the alarm, refer to the "Major Internal Audit Failure—Audit (6)" section on page 2-21.

Table 2-7 Audit (6) Details

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 the data field.
Primary Action	See the data field.

Audit (7)

Table 2-8 lists the details of the Audit (7) minor alarm. To troubleshoot and correct the cause of the alarm, refer to the "Minor Internal Audit Failure—Audit (7)" section on page 2-22.

Table 2-8 Audit (7) Details

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 the data field.
Primary Action	See the data field.

Audit (8)

Table 2-9 lists the details of the Audit (8) warning event. To monitor and correct the cause of the event, refer to the "Warning From Internal Audit—Audit (8)" section on page 2-17.

Table 2-9 Audit (8) Details

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 the data field.
Primary Action	See the data field.

Audit (9)

Audit (9) is not used.

Audit (10)

Table 2-10 lists the details of the Audit (10) information event. For additional information, refer to the "Call Data Audit Complete—Audit (10)" section on page 2-17.

Table 2-10 Audit (10) Details

Description	Call Data Audit Complete
Severity	Information
Threshold	100
Throttle	0
Datawords	Audit Information—STRING [256]
Primary Cause	A memory audit has been completed.
Primary Action	Check if any call blocks are freed as a result of the audit. An investigation to determine the root cause may be useful.

Audit (11)

Table 2-11 lists the details of the Audit (11) critical alarm. To troubleshoot and correct the cause of the alarm, refer to the "Critical Network Time Protocol Service Failure—Audit (11)" section on page 2-22.

Table 2-11 Audit (11) Details

Description	Critical Network Time Protocol Service Failure (Critical NTP Service Failure)
Severity	Critical
Threshold	100
Throttle	0
Datawords	Failure Details—STRING [220] Probable Causes—STRING [80] Corrective Actions—STRING [80]
Primary Cause	See the data field.
Primary Action	See the data field.

Audit (12)

Table 2-12 lists the details of the Audit (12) major alarm. To troubleshoot and correct the cause of the alarm, refer to the "Major Network Time Protocol Service Failure—Audit (12)" section on page 2-22.

Table 2-12 Audit (12) Details

Description	Major Network Time Protocol Service Failure (Major NTP Service Failure)
Severity	Major
Threshold	100
Throttle	0
Datawords	Failure Details—STRING [220] Probable Causes—STRING [80] Corrective Actions—STRING [80]
Primary Cause	See the data field.
Primary Action	See the data field.

Audit (13)

Table 2-13 lists the details of the Audit (13) minor alarm. To troubleshoot and correct the cause of the alarm, refer to the "Minor Network Time Protocol Service Failure—Audit (13)" section on page 2-23.

Table 2-13 Audit (13) Details

Description	Minor Network Time Protocol Service Failure (Minor NTP Service Failure)
Severity	Minor
Threshold	100
Throttle	0
Datawords	Failure Details—STRING [220] Probable Causes—STRING [80] Corrective Actions—STRING [80]
Primary Cause	See the data field.
Primary Action	See the data field.

Audit (14)

Table 2-14 lists the details of the Audit (14) warning event. To monitor and correct the cause of the event, refer to the "Network Time Protocol Service Warning—Audit (14)" section on page 2-18.

Table 2-14 Audit (14) Details

Description	Network Time Protocol Service Warning (NTP Service Warning)
Severity	Warning
Threshold	100
Throttle	0
Datawords	Failure Details—STRING [220] Probable Causes—STRING [80] Corrective Actions—STRING [80]
Primary Cause	See the data field.
Primary Action	See the data field.

Audit (15)

Table 2-15 lists the Audit (15) critical alarm details. To troubleshoot and correct the cause of the alarm, refer to the "Critical Index Shared Memory Error—Audit (15)" section on page 2-23.

Table 2-15 Audit (15) Details

Description	Critical Index Shared Memory Error (Critical IDX 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 the data field.
Primary Action	See the data field.

Audit (16)

Table 2-16 lists the details of the Audit (16) minor alarm. 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 2-23.

Table 2-16 Audit (16) Details

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 has occurred due to high call traffic volume or maintenance operation.
Primary Action	Monitor the heap usage frequently and see whether it is approaching the major threshold level.

Audit (17)

Table 2-17 lists the details of the Audit (17) major alarm. 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 2-24.

Table 2-17 Audit (17) Details

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 has occurred due to high call traffic volume, maintenance operation, or software problem.
Primary Action	Schedule a switchover during a maintenance window.

Audit (18)

Table 2-18 lists the details of the Audit (18) critical alarm. 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 2-24.

Table 2-18 Audit (18) Details

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 has occurred due to high call traffic volume, maintenance operation, or software problem.
Primary Action	Schedule a switchover during a maintenance window as soon as possible.

Audit (19)

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

Table 2-19 Audit (19) Details

Description	Recovered Memory of Stale Call
Severity	Warning
Threshold	20
Throttle	0
Datawords	Stale Memory Release Info—STRING [128]
Primary Cause	A loss of communication with originating or terminating side has occurred.
Primary Action	Check to see if adjacent network element is up and has a proper communication link with the Cisco BTS 10200.
Secondary Cause	Adjacent network device protocol error has occurred.
Secondary Action	Check the adjacent network device protocol compatibility.
Ternary Cause	An internal software error has occurred.
Ternary Action	Contact Cisco TAC.

Audit (20)

Table 2-20 lists the details of the Audit (20) major alarm. To troubleshoot and correct the cause of the alarm, refer to the "Audit Found Lost Call Data Record—Audit (20)" section on page 2-24.

Table 2-20 Audit (20) Details

Description	Audit Found Lost Call Data Record
Severity	Major
Threshold	20
Throttle	0
Datawords	Error Text—STRING [200]
Primary Cause	A software error has occurred. However, the orphaned records are recovered on detection 2d.
Primary Action	Contact Cisco TAC.

Audit (21)

Table 2-21 lists the details of the Audit (21) informational event. To monitor and correct the cause of the event, refer to the "Quality of Service Gate Memory Audit Complete—Audit (21)" section on page 2-19.

Table 2-21 Audit (21) Details

Description	Quality of Service Gate Memory Audit Complete (QoS Gate Memory Audit Complete)
Severity	Information
Threshold	100
Throttle	0
Datawords	Num Records Audited—FOUR_BYTES Audit Start Time—STRING [64]
Primary Cause	A gate memory audit has been completed.
Primary Action	Check to see if any gate memory was freed as a result of the audit. An investigation to determine the root cause may be useful.

Audit (22)

Table 2-22 lists the details of the Audit (22) informational event. To monitor and correct the cause of the event, refer to the "Quality of Service Gate Status Audit Complete—Audit (22)" section on page 2-19.

Table 2-22 Audit (22) Details

Description	Quality of Service Gate Status Audit Complete (QoS Gate Status Audit Complete)
Severity	Information
Threshold	100
Throttle	0
Datawords	Num Records Audited—FOUR_BYTES Audit Start Time—STRING [64]
Primary Cause	A gate status audit has been completed.
Primary Action	Check to see if any gate is removed from the cable modem termination system (CMTS) before the connection is released.

Audit (23)

Table 2-23 lists the details of the Audit (23) warning event. To monitor and correct the cause of the event, refer to the "Recover Memory of Dangling Gate—Audit (23)" section on page 2-20.

Table 2-23 Audit (23) Details

Description	Recover Memory of Dangling Gate
Severity	Warning
Threshold	100
Throttle	0
Datawords	Recovered Gate IDX—EIGHT_BYTES
Primary Cause	A software error has occurred.
Primary Action	If situation persists, contact Cisco TAC.

Audit (24)

Table 2-24 lists the details of the Audit (24) warning event. To monitor and correct the cause of the event, refer to the "No Gate in the Cable Modem Termination System for Active Connection—Audit (24)" section on page 2-20.

Table 2-24 Audit (24) Details

Description	No Gate in the Cable Modem Termination System for Active Connection (No Gate in CMTS for Active Connection)
Severity	Warning
Threshold	100
Throttle	0
Datawords	AGGR ID—STRING [16] Subscriber IP Address—STRING [32] Gate Direction—STRING [16]
Primary Cause	A communication error between the packet cable network components has occurred.
Primary Action	If situation persists, contact Cisco TAC.

Audit (25)

Table 2-25 lists the details of the Audit (25) major alarm. To troubleshoot and correct the cause of the alarm, refer to the "Core File Present—Audit (25)" section on page 2-25.

Table 2-25 Audit (25) Details

Description	Core File Present
Severity	Major
Threshold	100
Throttle	0
Datawords	Name of Host Machine—STRING [32] Directory Containing Core Files—STRING [128] Number of Core Files From 0 to 1—FOUR_BYTES Number of Core Files From 1 to 2—FOUR_BYTES Number of Core Files Greater Than 2—FOUR_BYTES Remaining Free File Space in MB—FOUR_BYTES
Primary Cause	A network element process has crashed.
Primary Action	Move the core file to a file server.

Monitoring Audit Events

This section provides the information you need to monitor and correct audit events. Table 2-26 lists all of the audit events in numerical order and provides cross-references to the subsections in this section.

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

Table 2-26 Cisco BTS 10200 Audit Events

Event Type	Event Name	Event Severity
Audit (1)	Test Report—Audit (1)	Information
Audit (2)	Start or Stop of Signaling System 7—Circuit Identification Code Audit—Audit (2)	Information
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 (10)	Call Data Audit Complete—Audit (10)	Information
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
Audit (21)	Quality of Service Gate Memory Audit Complete—Audit (21)	Information
Audit (22)	Quality of Service Gate Status Audit Complete—Audit (22)	Information
Audit (23)	Recover Memory of Dangling Gate—Audit (23)	Warning
Audit (24)	No Gate in the Cable Modem Termination System for Active Connection—Audit (24)	Warning
Audit (25)	Core File Present—Audit (25)	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 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 Cisco BTS 10200 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.

Sample 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 2-21.

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 2-21.

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 2-22.

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.

Call Data Audit Complete—Audit (10)

The Call Data Audit Complete event serves as an informational alert that a call data memory audit 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.

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 2-22.

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 2-22.

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 2-23.

Network Time Protocol Service Warning—Audit (14)

The Network Time Protocol Service Warning event serves as a warning that a problem with an 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.

To gather additional troubleshooting information, use the following:

From EMS:

```
show ems
```

From UNIX prompt:

```
/opt/BTSxntp/bin/ntpq -c peers
/opt/BTSxntp/bin/ntpq -c lpeers
/opt/BTSxntp/bin/ntpq -c lopeers
/opt/BTSxntp/bin/ntpq -c opeers
cat /etc/inet/ntp.conf
```

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 2-23.

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 2-23.

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 2-24.

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 2-24.

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 the originating or terminating side occurred. To correct the primary cause of the warning, check to see if the adjacent network element link is up and that the adjacent network element is properly communicating with the Cisco BTS 10200. 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. The ternary cause of the warning is an internal software error. If a internal software error has occurred, contact Cisco TAC to obtain technical assistance. Prior to contacting Cisco TAC, collect a trace log corresponding to the time of the alarm.

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 2-24.

Quality of Service Gate Memory Audit Complete—Audit (21)

The Quality of Service Gate Memory Audit Complete event serves as an informational alert that a quality of service gate memory audit has been completed. To correct the primary cause of the event, check to see if any gate memory was freed as a result of the audit. An investigation to determine the root cause may be useful.

Quality of Service Gate Status Audit Complete—Audit (22)

The Quality of Service Gate Status Audit Complete event serves as an informational alert that a quality of service gate status audit has been completed. To correct the primary cause of the event, check to see if any gate was removed in the CMTS before the connection is released.

Recover Memory of Dangling Gate—Audit (23)

The Recover Memory of Dangling Gate event serves as a warning that the memory recovery of a dangling gate has occurred. The primary cause of the warning is that a software error has occurred. If the situation persists, contact Cisco to obtain technical assistance.

Prior to contacting Cisco TAC, collect a Cisco BTS 10200 trace log corresponding to the time of the event and collect the following additional information from the CMTS.

```
show packetcable gate summary
show packetcable gate <gate id>
```

No Gate in the Cable Modem Termination System for Active Connection—Audit (24)

The No Gate in the Cable Modem Termination System for Active Connection event serves as a warning that no gate in the CMTS is available for the active connection. The primary cause of the warning is that a communication error has occurred between packet cable network components. If the situation persists, contact Cisco to obtain technical assistance.

Prior to contacting Cisco TAC, collect a Cisco BTS 10200 trace log corresponding to the time of the event and collect the following additional information from the CMTS.

```
show packetcable global
show packetcable gate summary
```

Core File Present—Audit (25)

The Core File Present alarm (major) indicates that a network element process has crashed. To troubleshoot and correct the cause of the Core File Present alarm, refer to the "Core File Present—Audit (25)" section on page 2-25.

Troubleshooting Audit Alarms

This section provides the information you need to troubleshoot and correct audit alarms. Table 2-27 lists all of the audit alarms in numerical order and provides cross-references to the subsections in this section.

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

Table 2-27 Cisco BTS 10200 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
Audit (25)	Core File Present—Audit (25)	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 Failure Details data field and Probable Causes data field datawords. For the corrective actions for the alarm, review the Corrective Actions data field dataword and take 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 and 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 and take the corrective actions listed.

Use the following command to gather additional troubleshooting information from the EMS.

```
show ems
```

From the UNIX prompt, use the following commands to gather additional troubleshooting information from the EMS.

```
/opt/BTSxntp/bin/ntpq -c peers
/opt/BTSxntp/bin/ntpq -c lpeers
/opt/BTSxntp/bin/ntpq -c lopeers
/opt/BTSxntp/bin/ntpq -c opeers
cat /etc/inet/ntp.conf
```

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 and proceed with the corrective actions listed.

Use the following command to gather additional troubleshooting information from the EMS.

```
show ems
```

From the UNIX prompt, use the following commands to gather additional troubleshooting information from the EMS.

```
/opt/BTSxntp/bin/ntpq -c peers
/opt/BTSxntp/bin/ntpq -c lpeers
/opt/BTSxntp/bin/ntpq -c lopeers
/opt/BTSxntp/bin/ntpq -c opeers
cat /etc/inet/ntp.conf
```

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 and proceed with the corrective actions listed.

To gather additional troubleshooting information, use the following:

Use the following command to gather additional troubleshooting information from the EMS.

```
show ems
```

From the UNIX prompt, use the following commands to gather additional troubleshooting information from the EMS.

```
/opt/BTSxntp/bin/ntpq -c peers
/opt/BTSxntp/bin/ntpq -c lpeers
/opt/BTSxntp/bin/ntpq -c lopeers
/opt/BTSxntp/bin/ntpq -c opeers
cat /etc/inet/ntp.conf
```

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 and 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. Monitor the heap usage and check to see if it is approaching the major threshold level.

From UNIX prompt, use the following commands to show the process heap memory usage.

```
date
show_heap <pid of mga> > /opt/mga_heap.txt
```

The **show_heap** command is not on the system by default. To obtain the show_heap tool, contact Cisco TAC.

Note Heap memory usage is automatically monitored once per hour.

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 increase in heap usage is a high call volume of traffic, a maintenance operation, or a software problem. To isolate and correct the primary cause of the alarm, schedule a switchover during a maintenance window.

From UNIX prompt, use the following commands to show the process heap memory usage.

```
date
show_heap <pid of mga> > /opt/mga_heap.txt
```

The **show_heap** command is not on the system by default. To obtain the show_heap tool, contact Cisco TAC.

Note Heap memory usage is automatically monitored once per hour.

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, or a software problem. To isolate and correct the primary cause of the alarm, schedule a switchover during a maintenance window as soon as possible.

From the UNIX, prompt use the following commands to show the process heap memory usage,

```
date
show_heap <pid of mga> > /opt/mga_heap.txt
```

The **show_heap** command is not on the system by default. To obtain the show_heap tool contact Cisco TAC.

Note Heap memory usage is automatically monitored once per hour.

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. Prior to contacting Cisco TAC, collect a trace log corresponding to the time of the alarm.

Core File Present—Audit (25)

The Core File Present alarm (major) indicates that a network element process has crashed and that the Cisco BTS 10200 system has created a core file to assist in determining the root cause of the network element process crash. To correct the primary cause of the alarm, move the core file to a file server.

Note Although the Cisco BTS 10200 software directs its core files to the directory /bin, core files generated by software that is not Cisco BTS 10200 software (such as the platform operating system), are stored in the /opt/core directory. When a core dump occurs that is not generated by the Cisco BTS 10200, the Cisco BTS 10200 issues an Audit 25 alarm, as it does for Cisco BTS 10200 core dumps, to indicate that such an incident occurred.

To move the core file to an FTP server, run the following commands:

```
pstack <corefile>
ftp core file to ftp-sj.cisco.com/incoming
```

Once the core files is moved to the file server (FTP server), contact Cisco TAC.

CHAPTER 3

Billing Troubleshooting

Revised: August 10, 2011, OL-25016-01

Introduction

This chapter provides the information needed for monitoring and troubleshooting 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 for monitoring and correcting the billing events
- Troubleshooting Billing Alarms—Provides the information needed for troubleshooting and correcting the 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; the events and alarms are arranged in numerical order. Table 3-1 lists all of the billing events and alarms by severity.

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

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	Information	Not Used
Billing (4)	Billing (3)	Billing (2)	Billing (14)	Billing (1)	Billing (9)
Billing (7)	Billing (6)	Billing (40)	Billing (42)	Billing (5)	Billing (10)
Billing (13)	Billing (8)	Billing (41)		Billing (36)	Billing (11)
Billing (35)	Billing (15)	Billing (45)		Billing (57)	Billing (12)
Billing (49)	Billing (29)	Billing (46)		Billing (59)	Billing (16)
Billing (52)	Billing (30)	Billing (47)			Billing (17)
Billing (55)	Billing (31)	Billing (53)			Billing (18)
Billing (56)	Billing (32)				Billing (19)
	Billing (33)				Billing (20)
	Billing (37)				Billing (21)
	Billing (38)				Billing (22)
	Billing (44)				Billing (23)
	Billing (48)				Billing (24)
	Billing (54)				Billing (25)
	Billing (58)				Billing (26)
	Billing (60)				Billing (27)
					Billing (28)
					Billing (34)
					Billing (39)
					Billing (43)
					Billing (50)
					Billing (51)

Billing (1)

Table 3-2 lists the details of the Billing (1) informational event. For additional information, refer to the "Test Report—Billing (1)" section on page 3-27.

Table 3-2 Billing (1) Details

Description	Test Report
Severity	Information
Threshold	10000
Throttle	0

Billing (2)

Table 3-3 lists the details of the Billing (2) minor alarm. To troubleshoot and correct the cause of the alarm, refer to the "Billing Partition Disk Usage Minor Threshold Exceeded—Billing (2)" section on page 3-35.

Table 3-3 Billing (2) Details

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 process should catch up to the write process within a few minutes, and the alarm should not remain active.
Secondary Cause	Some fluctuation in disk usage is to be expected as the 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 the call volume, and then step downward (critical to major to minor) when the 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 the commands.

Billing (3)

Table 3-4 lists the details of the Billing (3) major alarm. To troubleshoot and correct the cause of the alarm, refer to the "Billing Partition Disk Usage Major Threshold Exceeded—Billing (3)" section on page 3-35.

Table 3-4 Billing (3) Details

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 process should catch up to the write process within a few minutes, and the alarm should not remain active.
Secondary Cause	Some fluctuation in disk usage is to be expected as the 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 the call volume, and then step downward (critical to major to minor) when the 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 the 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.

Billing (4)

Table 3-5 list the details of the Billing (4) critical alarm. To troubleshoot and correct the cause of the alarm, refer to the "Billing Partition Disk Usage Critical Threshold Exceeded—Billing (4)" section on page 3-36.

Table 3-5 Billing (4) Details

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 process should catch up to the write process within a few minutes, and the alarm should not remain active.
Secondary Cause	Some fluctuation in disk usage is to be expected as the 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 the call volume, and then step downward (critical to major to minor) when the 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.

Billing (5)

Table 3-6 lists the details of the Billing (5) informational event. For additional information, refer to the "Billing Partition Disk Usage Within Normal Range—Billing (5)" section on page 3-28.

Table 3-6 Billing (5) Details

Description	Billing Partition Disk Usage Within Normal Range
Severity	Information
Threshold	100
Throttle	0
Datawords	Disk Usage Percentage—TWO_BYTES

Billing (6)

Table 3-7 list the details of the Billing (6) major alarm. 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 3-36.

Table 3-7 Billing (6) Details

Description	File Transfer Protocol/Secure File Transfer Protocol Transfer Failed (FTP/SFTP Transfer Failed)
Severity	Major
Threshold	100
Throttle	0
Datawords	TransferType—STRING [5] FileName—STRING [40] RemoteAddress—STRING [40] Error—STRING [50]
Primary Cause	Unable to connect to the remote host.
Primary Action	Verify that the remote host is reachable. Run the **show billing-acct-addr** command and verify that the billing-server-addr is correct. Change the billing-server-addr, if necessary, using the change **billing-acct-addr** command.
Secondary Cause	Unable to log in to the remote host.
Secondary Action	Use **show billing-acct-addr** command to verify that the user-name is a valid user for the host specified in the billing-server-addr. If user-name is correct and the TransferType dataword shows File Transfer Protocol (FTP), reenter the password using the **change billing-acct-addr** command. If user-name is correct and the TransferType dataword shows Secure File Transfer Protocol (SFTP), verify that secure shell (SSH) keys have been preconfigured for the user name on both the Cisco BTS 10200 and the remote host.
Ternary Cause	A file transfer error has occurred.
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 and the remote host.
Subsequent Cause	The CDB_BILLING_SUPP flag is not set to Y in the call-agent-profile table.
Subsequent Action	Verify that the CDB_BILLING_SUPP flag is set to Y in the call-agent-profile table.

Billing (7)

Table 3-8 lists the details of the Billing (7) critical alarm. To troubleshoot and correct the cause of the alarm, refer to the "Transmission Control Protocol Connection Error—Billing (7)" section on page 3-37.

Table 3-8 Billing (7) Details

Description	Transmission Control Protocol Connection Error (TCP Connection Error)
Severity	Critical
Threshold	100
Throttle	0
Datawords	Hostname—STRING [100]
Primary Cause	A system call error has occurred.
Primary Action	Check the address in platform configuration.
Secondary Cause	The Cisco BTS 10200 is not connected to the right address.
Secondary Action	Contact Cisco TAC.

Billing (8)

Table 3-9 lists the details of the Billing (8) major alarm. To troubleshoot and correct the cause of the alarm, refer to the "Transmission Control Protocol Packet Receive Failure—Billing (8)" section on page 3-37.

Table 3-9 Billing (8) Details

Description	Transmission Control Protocol Packet Receive Failure (TCP Packet Receive Failure)
Severity	Major
Threshold	100
Throttle	0
Datawords	Host Name—STRING [25]
Primary Cause	Peer went down; socket closed.
Primary Action	Check the peer status and bring the peer back up.

Billing (9)

Billing (9) is not used.

Billing (10)

Billing (10) is not used.

Billing (11)

Billing (11) is not used.

Billing (12)

Billing (12) is not used.

Billing (13)

Table 3-10 lists the details of the Billing (13) critical alarm. To troubleshoot and correct the cause of the alarm, refer to the "Database Connection Error—Billing (13)" section on page 3-38.

Table 3-10 Billing (13) Details

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, contact Cisco TAC.

Billing (14)

Table 3-11 lists the details of the Billing (14) warning event. To monitor and correct the cause of the event, refer to the "File Open Error—Billing (14)" section on page 3-29.

Table 3-11 Billing (14) Details

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	Contact Cisco TAC.

Billing (15)

Table 3-12 lists the details of the Billing (15) major alarm. To troubleshoot and correct the cause of the alarm, refer to the "File Write Error—Billing (15)" section on page 3-38.

Table 3-12 Billing (15) Details

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	Contact Cisco TAC.

Billing (16)

Billing (16) is not used.

Billing (17)

Billing (17) is not used.

Billing (18)

Billing (18) is not used.

Billing (19)

Billing (19) is not used.

Billing (20)

Billing (20) is not used.

Billing (21)

Billing (21) is not used.

Billing (22)

Billing (22) is not used.

Billing (23)

Billing (23) is not used.

Billing (24)

Billing (24) is not used.

Billing (25)

Billing (25) is not used.

Billing (26)

Billing (26) is not used.

Billing (27)

Billing (27) is not used.

Billing (28)

Billing (28) is not used.

Billing (29)

Table 3-13 lists the details of the Billing (29) major alarm. To troubleshoot and correct the cause of the alarm, refer to the "Call Data Block Send Failed—Billing (29)" section on page 3-38.

Table 3-13 Billing (29) Details

Description	Call Data Block Send Failed (CDB Send Failed)
Severity	Major
Threshold	100
Throttle	0
Primary Cause	Transmission Control Protocol (TCP) send call failure.
Primary Action	Check the port number and address of the blg and bmg processes in the platform.cfg file.
Secondary Cause	Both the EMS servers are down.
Secondary Action	Check if both EMS servers are down. If they are, bring at least one up.

Billing (30)

Table 3-14 lists the details of the Billing (30) major alarm. To troubleshoot and correct the cause of the alarm, refer to the "Domain Name Mapping Failed—Billing (30)" section on page 3-38.

Table 3-14 Billing (30) Details

Description	Domain Name Mapping Failed
Severity	Major
Threshold	100
Throttle	0
Datawords	Address—STRING [50]
Primary Cause	Wrong domain name system (DNS) name mapping specified in the configuration files.
Primary Action	Check the opticall.cfg and platform.cfg for the right mapping.

Billing (31)

Table 3-15 lists the details of the Billing (31) major alarm. To troubleshoot and correct the cause of the alarm, refer to the "Port Not Specified—Billing (31)" section on page 3-38.

Table 3-15 Billing (31) Details

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)

Table 3-16 lists the details of the Billing (32) major alarm. To troubleshoot and correct the cause of the alarm, refer to the "Element Management System Address Not Specified—Billing (32)" section on page 3-39.

Table 3-16 Billing (32) Details

Description	Element Management System Address not Specified (EMS Address not Specified)
Severity	Major
Threshold	100
Throttle	0
Primary Cause	Either the primary or secondary EMS address has not been specified in the platform.cfg file.
Primary Action	Check the platform.cfg for the process Billing (BLG) and add the missing addresses to the file.

Billing (33)

Table 3-17 lists the details of the Billing (33) major alarm. 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 3-39.

Table 3-17 Billing (33) Details

Description	File Transfer Protocol/Secure File Transfer Protocol Parameters Invalid (FTP/SFTP Parameters Invalid)
Severity	Major
Threshold	100
Throttle	0
Datawords	TransferType—STRING [5] BillingServerDir—STRING [100] BillingServerAddr—STRING [100] User Name—STRING [100]
Primary Cause	The billing-acct-addr table is not fully provisioned with the information needed to perform file transfers.
Primary Action	Check billing-acct-addr fields using the **show billing-acct-addr** command. For FTP file transfer, ensure that the billing-server-addr, billing-server-directory, user-name, and password (not displayed) are provisioned. Also ensure that sftp-supp is set to N. For SFTP file transfer, ensure that the billing-server-addr, billing-server-directory, and user-name are provisioned. Also ensure that sftp-supp is set to Y.

Billing (34)

Billing (34) is not used.

Billing (35)

Table 3-18 lists the details of the Billing (35) critical alarm. To troubleshoot and correct the cause of the alarm, refer to the "All Billing Links at Billing Server Down—Billing (35)" section on page 3-39.

Table 3-18 Billing (35) Details

Description	All Billing Links at Billing Server Down
Severity	Critical
Threshold	100
Throttle	0
Primary Cause	The cable connection might have been pulled out.
Primary Action	Restore the cable connection.
Secondary Cause	An **ifconfig down** command might have been executed on the interfaces.
Secondary Action	Execute an **ifconfig up** command on the interfaces.

Billing (36)

Table 3-19 lists the details of the Billing (36) informational event. For additional information, refer to the "Billing Link Restored—Billing (36)" section on page 3-30.

Table 3-19 Billing (36) Details

Description	Billing Link Restored
Severity	Information
Threshold	100
Throttle	0
Datawords	Interface Name—STRING [50]
Primary Cause	The cable connection has been restored.
Primary Action	None

Billing (37)

Table 3-20 lists the details of the Billing (37) major alarm. To troubleshoot and correct the cause of the alarm, refer to the "Billing Link Failure—Billing (37)" section on page 3-39.

Table 3-20 Billing (37) Details

Description	Billing Link Failure
Severity	Major
Threshold	100
Throttle	0
Datawords	Interface Name—STRING [5]
Primary Cause	The cable connection may have been pulled.
Primary Action	Restore the cable connection.
Secondary Cause	An **ifconfig down** command may have been performed on the interface.
Secondary Action	Perform an **ifconfig up** command on the interface.

Billing (38)

Table 3-21 lists the details of the Billing (38) major alarm. To troubleshoot and correct the cause of the alarm, refer to the "Event Message Log File Access Error—Billing (38)" section on page 3-39.

Table 3-21 Billing (38) Details

Description	Event Message Log File Access Error (EM Log File Access Error)
Severity	Major
Threshold	50
Throttle	0
Datawords	Type of Access Error—STRING [25] Reason for Error—STRING [40] Sequence Number OFF—FOUR_BYTES Index of Event Messa—FOUR_BYTES Location Tag—STRING [30]
Primary Cause	System error, may be out of file descriptors.
Primary Action	Contact Cisco TAC.
Secondary Cause	The disk may be faulty.
Secondary Action	Make the Bulk Data Management System (BDMS) switch over to its mate node.

Billing (39)

Billing (39) is not used.

Billing (40)

Table 3-22 lists the details of the Billing (40) minor alarm. To troubleshoot and correct the cause of the alarm, refer to the "Event Message Encode Failure—Billing (40)" section on page 3-40.

Table 3-22 Billing (40) Details

Description	Event Message Encode Failure (EM Encode Failure)
Severity	Minor
Threshold	100
Throttle	0
Datawords	Location Tag—STRING [30]
Primary Cause	There is a problem with the format of the data to be sent to the record keeping system (RKS).
Primary Action	If problem persists, contact Cisco TAC.

Billing (41)

Table 3-23 lists the details of the Billing (41) minor alarm. To troubleshoot and correct the cause of the alarm, refer to the "Message Content Error—Billing (41)" section on page 3-40.

Table 3-23 Billing (41) Details

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	Contact Cisco TAC.

Billing (42)

Table 3-24 list the details of the Billing (42) warning event. To monitor and correct the cause of the event, refer to the "Error Reading Provisioned Data—Using Default—Billing (42)" section on page 3-31.

Table 3-24 Billing (42) Details

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	An application was unable to read the provisioned data, and had to resort to using default values.
Primary Action	Check to ensure that a complete load has been installed on the system. If the load is complete and problem persists, contact Cisco TAC.

Billing (43)

Billing (43) is not used.

Billing (44)

Table 3-25 lists the details of the Billing (44) major alarm. To troubleshoot and correct the cause of the alarm, refer to the "Record Keeping System Switch Occurred—Billing (44)" section on page 3-40.

Table 3-25 Billing (44) Details

Description	Record Keeping System Switch Occurred (RKS Switch Occurred)
Severity	Major
Threshold	100
Throttle	0
Datawords	Type of RKS Switch—STRING [20] Location Tag—STRING [30]
Primary Cause	Billing changed the destination RKS to which event messages are transmitted. 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)

Table 3-26 lists the details of the Billing (45) minor alarm. To troubleshoot and correct the cause of the alarm, refer to the "Event Message Log File Opened—Billing (45)" section on page 3-40.

Table 3-26 Billing (45) Details

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)

Table 3-27 lists the details of the Billing (46) minor alarm. To troubleshoot and correct the cause of the alarm, refer to the "Event Message Log File Closed—Billing (46)" section on page 3-40.

Table 3-27 Billing (46) Details

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)

Table 3-28 lists the details of the Billing (47) minor alarm. To troubleshoot and correct the cause of the alarm, refer to the "Record Keeping System Unreachable for One Hour—Billing (47)" section on page 3-40.

Table 3-28 Billing (47) Details

Description	Record Keeping System Unreachable for One Hour (RKS Unreachable for 1 Hour)
Severity	Minor
Threshold	25
Throttle	0
Datawords	Location Tag—STRING [30]
Primary Cause	Billing has not been able to communicate with any RKS for the past hour.
Primary Action	Check status of the primary and secondary RKS servers; 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.

Billing (48)

Table 3-29 lists the details of the Billing (48) major alarm. To troubleshoot and correct the cause of the alarm, refer to the "Record Keeping System Unreachable for Three Hours—Billing (48)" section on page 3-41.

Table 3-29 Billing (48) Details

Description	Record Keeping System Unreachable for Three Hours (RKS Unreachable for 3 Hours)
Severity	Major
Threshold	25
Throttle	0
Datawords	Location Tag—STRING [30]
Primary Cause	Billing has not been able to communicate with any RKS for the past three hours.
Primary Action	Check status of the primary and secondary RKS servers: attempt to bring them into service. Verify that the radius-profile table and call-agent-profile table are provisioned such that communication with the RKS servers is possible.

Billing (49)

Table 3-30 lists the details of the Billing (49) critical alarm. To troubleshoot and correct the cause of the alarm, refer to the "Record Keeping System Unreachable for Five Hours—Billing (49)" section on page 3-41.

Table 3-30 Billing (49) Details

Description	Record Keeping System Unreachable for 5 Hours (RKS 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 that the radius-profile table and call-agent-profile table are provisioned such that communication with the RKS servers is possible.

Billing (50)

Billing (50) is not used.

Billing (51)

Billing (51) is not used.

Billing (52)

Table 3-31 lists the details of the Billing (52) critical alarm. 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 3-41.

Table 3-31 Billing (52) Details

Description	Bulk Data Management System Stopped Generating New Billing File (BDMS Stopped Generating New Billing File)
Severity	Critical
Threshold	100
Throttle	0
Primary Cause	Call detail records are accumulating on the disk associated with the billing files in the EMS. This is because data is being written into the billing files faster than it is being forwarded to the Billing Mediation Server. The FTP to the Billing Mediation Server may not be working. The maximum disk partition for billing records 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 errors 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, and BDMS needs to be restarted before it will start generating new billing files.

Billing (53)

Table 3-32 lists the details of the Billing (53) minor alarm. To troubleshoot and correct the cause of the alarm, refer to the "Event Message Disk Space 50 Percent Full—Billing (53)" section on page 3-41.

Table 3-32 Billing (53) Details

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	The event message storage has reached 50% of the maximum storage allowed.
Primary Action	Move the event message files out of the specified directory. Store them in another location, or discard them.

Billing (54)

Table 3-33 lists the details of the Billing (54) major alarm. To troubleshoot and correct the cause of the alarm, refer to the "Event Message Disk Space 70 Percent Full—Billing (54)" section on page 3-41.

Table 3-33 Billing (54) Details

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	The event message storage has reached 70% of the maximum storage allowed.
Primary Action	Move the event message files out of the specified directory. Store them in another location, or discard them.

Billing (55)

Table 3-34 lists the details of the Billing (55) critical alarm. To troubleshoot and correct the cause of the alarm, refer to the "Event Message Disk Space 100 Percent Full—Billing (55)" section on page 3-42.

Table 3-34 Billing (55) Details

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	The 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 the event message files out of the specified directory. Store them in another location, or discard them.

Billing (56)

Table 3-35 lists the details of the Billing (56) critical alarm. To troubleshoot and correct the cause of the alarm, refer to the "Billing Data Corruption Detected—Billing (56)" section on page 3-42.

Table 3-35 Billing (56) Details

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	The billing data stored on the 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.

Billing (57)

Table 3-36 lists the details of the Billing (57) informational event. For additional information, refer to the "Prepaid Subscriber Call Attempt Failed Because of Balance—Billing (57)" section on page 3-33.

Table 3-36 Billing (57) Details

Description	Prepaid Subscriber Call Attempt Failed Because of Balance
Severity	Information
Threshold	100
Throttle	0
Datawords	Instance Name—STRING [65] Calling Party—STRING [32] Called Party—STRING [32] Pop ID- STRING [32]
Primary Cause	The subscriber has consumed the balance on his or her account.
Primary Action	Ask the subscriber to deposit money in the account.
Secondary Cause	There may be a problem in the billing information at prepaid server.
Secondary Action	Verify the billing info at the prepaid server.

Billing (58)

Table 3-37 lists the details of the Billing (58) major alarm. To troubleshoot and correct the cause of the alarm, refer to the "Signaling Prepaid Server Inaccessible—Billing (58)" section on page 3-42.

Table 3-37 Billing (58) Details

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 of the prepaid servers are down.
Primary Action	Check and correct the operating status of the prepaid servers.
Secondary Cause	The Internet Protocol (IP) network between the Cisco BTS 10200 plain old telephone service (POTS) Feature Server (FS) and the prepaid servers is down.
Secondary Action	Check and correct any problems in the IP network.

Billing (59)

Table 3-38 lists the details of the Billing (59) informational event. For additional information, refer to the "Billing File Name Type Change in Command Line Interface Is Inconsistent—Billing (59)" section on page 3-33.

Table 3-38 Billing (59) Details

Description	Billing File Name Type Change in the Command Line Interface is Inconsistent
Severity	Information
Threshold	100
Throttle	0
Primary Cause	A user updated the billing file name type in the CLI.
Primary Action	Execute a switchover or a platform restart so the change is propagated to the billing code.

Billing (60)

Table 3-39 lists the details of the Billing (60) major alarm. To troubleshoot and correct the cause of the alarm, refer to the "Bad File Detected During Startup—Billing (60)" section on page 3-42.

Table 3-39 Billing (60) Details

Description	Bad File Detected During Startup
Severity	Major
Threshold	100
Throttle	0
Datawords	Filename of the Bad File—STRING [128] Diagnosis—STRING [64] Changed to Filename—STRING [128]
Primary Cause	A bad billing file was generated due to a CPU failure, power outage, ungraceful shutdown, or disk failure.
Primary Action	The billing subsystem isolates the bad file, renames the bad billing file, and continues to complete the initialization. The bad file is placed out of the control of the billing subsystem, and the billing subsystem will not FTP the bad file to the BMS. The bad file should 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 3-40 lists all of the billing events in numerical order and provides cross-references to the subsections in this section.

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

Table 3-40 Cisco BTS 0200 Billing Events

Event Type	Event Name	Event Severity
Billing (1)	Test Report—Billing (1)	Information
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)	Information
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)	Information
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

Table 3-40 Cisco BTS 0200 Billing Events (continued)

Event Type	Event Name	Event Severity
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
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)	Information
Billing (58)	Signaling Prepaid Server Inaccessible—Billing (58)	Major
Billing (59)	Billing File Name Type Change in Command Line Interface Is Inconsistent—Billing (59)	Information
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 3-35.

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 3-35.

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 3-36.

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 the 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 3-36.

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 3-37.

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 3-37.

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 3-38.

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 might be out of file descriptors. If a file open error has occurred, contact Cisco TAC to obtain technical assistance.

From the UNIX prompt, collect the following information prior to contacting Cisco TAC.

```
sysdef -i
df -k
```

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 3-38.

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 3-38.

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 3-38.

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 3-38.

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 3-39.

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 3-39.

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 3-39.

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 3-39.

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 3-39.

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 3-40.

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 3-40.

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

The Error Reading Provisioned Data—Using Default event functions as a warning that an error occurred during the reading of 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 system. If the load is complete and the problem persists, contact Cisco TAC.

Record Keeping System Switch Occurred—Billing (44)

The Record Keeping System Switch Occurred alarm (major) indicates that an 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 3-40.

Event Message Log File Opened—Billing (45)

The Event Message Log File Opened alarm (minor) indicates that an 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 3-40.

Event Message Log File Closed—Billing (46)

The Event Message Log File Closed alarm (minor) indicates that an 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 3-40.

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 1 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 3-40.

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 3 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 3-41.

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 5 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 Five Hours—Billing (49)" section on page 3-41.

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 3-41.

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 3-41.

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 3-41.

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 3-42.

Billing Data Corruption Detected—Billing (56)

The Billing Data Corruption Detected alarm (critical) indicates that 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 3-42.

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

The Prepaid Subscriber Call Attempt Failed Because of Balance event functions as an informational alert that a prepaid subscriber call attempt has failed because 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 his or her 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 3-42.

Billing File Name Type Change in Command Line Interface Is Inconsistent—Billing (59)

The Billing File Name Type Change in Command Line Interface Is Inconsistent event serves as an informational alert that a user updated the billing filename type in the CLI. To correct the primary cause of the event, execute a switchover or a platform restart so that the change is propagated to the billing code.

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 3-42.

Troubleshooting Billing Alarms

This section provides the information needed to troubleshoot and correct billing alarms. Table 3-41 lists all of the billing alarms in numerical order and provides cross-references to the subsections in this section.

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

Table 3-41 Cisco BTS 10200 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 Five Hours—Billing (49)	Critical

Table 3-41 Cisco BTS 10200 Billing Alarms (continued)

Alarm Type	Alarm Name	Alarm Severity
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 identify the primary cause of the alarm, monitor the alarm. The read should catch up to the 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.

For additional troubleshooting information, from the UNIX prompt collect **df -k**.

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 identify the primary cause of the alarm, monitor this alarm. The read should catch up to the 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.

Prior to contacting Cisco TAC, from the UNIX prompt collect **df -k** using the following commands.

```
df -k
du -sh /opt/bms/ftp/billing
```

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 identify the primary cause of the alarm, monitor this alarm. The read should catch up to the 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.

Prior to contacting Cisco TAC, from the UNIX prompt collect **df -k** using the following commands.

```
df -k
du -sh /opt/bms/ftp/billing
```

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 to the billing server has failed. The primary cause of the alarm is that the Cisco BTS 10200 is unable to connect to a remote host. To correct the primary cause of the alarm, first verify the remote host is reachable. Run the **show billing-acct-addr** command and verify that the billing-server-addr is correct. Change the billing-server-addr, if necessary, by using the **change billing-acct-addr** command. The secondary cause of the alarm is that the Cisco BTS 10200 is unable to log in to remote host. To correct the secondary cause of the alarm, first use the **show billing-acct-addr** command to verify that the user-name is a valid user for the host specified in the billing-server-addr. If the user-name is correct and the TransferType dataword shows FTP, reenter the password by using the **change billing-acct-addr** command. If the user-name is correct and the TransferType dataword shows SFTP, verify that SSH keys have been preconfigured for user-name on both the Cisco BTS 10200 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, first 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 and the remote host. The subsequent cause of the alarm is that the CDB_BILLING_SUPP flag is not set to Y in the call-agent-profile table. To correct the subsequent cause of the alarm, check and verify that the CDB_BILLING_SUPP flag is set to Y in the call-agent-profile table.

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

Use the following information to check the datawords:

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

- file name—The name of file that the Softswitch is attempting to send to the billing server.
- FTP address—The IP address/domain name of the billing server that the Cisco BTS 10200 is attempting to reach.
- error—One or more of the following data words can be displayed to indicate missing or incorrect information:
  - Log in—The username for the billing server is missing or incorrect in the database, or the user 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 log in username (for the billing server) is missing or incorrect in the database.
   b. The username is correct but the user 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 platform configuration. The secondary cause of the alarm is the Cisco BTS 10200 is not connected to the right address. To correct the secondary cause of the alarm, call Cisco TAC for technical support.

If the alarm is repeating, collect a packet capture between the Cisco BTS 10200 and the billing server prior to contacting Cisco TAC.

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.

Prior to contacting Cisco TAC, collect the following additional information.

From the EMS UNIX prompt, collect the following information:

```
ps -ef
nodestat
```

From the CLI prompt, collect the following information:

```
status system
```

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 system may be out of file descriptors. To correct the primary cause of the alarm, contact Cisco TAC for technical support.

Prior to contacting Cisco TAC, collect the following information from the UNIX prompt:

```
sysdef -i
df -k
```

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 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 the parameters have 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 by using the **show billing-acct-addr** command. For FTP file transfer, ensure that the billing-server-addr, billing-server-directory, user-name, and password (not displayed) are provisioned. Also ensure that the sftp-supp is set to N. For SFTP file transfer, ensure that the billing-server-addr, billing-server-directory, and user-name are provisioned. Also ensure that the 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 the 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 an **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 system may be out of file descriptors. To correct the primary cause of the alarm, contact Cisco TAC. 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.

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.

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 (the RKS to which event messages are transmitted). 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 an 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 an 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 1 hour. The primary cause of the alarm is that billing has not been able to communicate with any RKS for the past 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 3 hours. The primary cause of the alarm is that billing has not been able to communicate with any RKS for the past 3 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 Five Hours—Billing (49)

The Record Keeping System Unreachable for Five Hours alarm (critical) indicates that the RKS servers have been unreachable for 5 hours. The primary cause of the alarm is that billing has not been able to communicate with any RKS for the past 5 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. The FTP to the Billing Mediation Server may not be working. The maximum disk partition for billing records 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 the 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 are not forwarded or deleted automatically. In this case, files have to be manually deleted or moved out, and the BDMS needs to be restarted before it begins to generate 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 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.

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 POTS feature server (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 failure, 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 corrected, it remains on the system and is not automatically sent by FTP to the BMS system.

CHAPTER 4

Call Processing Troubleshooting

Revised: August 10, 2011, OL-25016-01

Introduction

This chapter provides the information needed for monitoring and troubleshooting 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 for monitoring and correcting the call processing events
- Troubleshooting Call Processing Alarms—Provides the information needed for troubleshooting and correcting the call processing alarms

For additional call processing routing and translation information, refer to the *Cisco BTS 10200 Softswitch Routing and Dial Plan Guide, Release 6.0.3*.

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; the event and alarms are arranged in numerical order. Table 4-1 lists all of the call processing events and alarms by severity.

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

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	Information	Not Used
Call Processing (12)		Call Processing (11)	Call Processing (8)	Call Processing (1)	Call Processing (2)
		Call Processing (38)	Call Processing (16)	Call Processing (9)	Call Processing (3)
		Call Processing (41)	Call Processing (17)	Call Processing (13)	Call Processing (4)
			Call Processing (18)	Call Processing (14)	Call Processing (5)
			Call Processing (19)	Call Processing (15)	Call Processing (6)
			Call Processing (20)	Call Processing (42)	Call Processing (7)
			Call Processing (21)	Call Processing (46)	Call Processing (10)
			Call Processing (22)		
			Call Processing (23)		
			Call Processing (24)		
			Call Processing (25)		
			Call Processing (26)		
			Call Processing (27)		
			Call Processing (28)		
			Call Processing (29)		
			Call Processing (30)		
			Call Processing (31)		
			Call Processing (32)		
			Call Processing (33)		
			Call Processing (34)		
			Call Processing (35)		
			Call Processing (36)		
			Call Processing (37)		
			Call Processing (39)		
			Call Processing (40)		
			Call Processing (43)		
			Call Processing (44)		

Table 4-1 Call Processing Events and Alarms by Severity (continued)

Critical	Major	Minor	Warning	Information	Not Used
			Call Processing (45)		
			Call Processing (47)		

Call Processing (1)

Table 4-2 lists the details of the Call Processing (1) informational event. For additional information, refer to the "Test Report—Call Processing (1)" section on page 4-27.

Table 4-2 Call Processing (1) Details

Description	Test Report
Severity	Information
Threshold	10000
Throttle	0

Call Processing (2)

Call Processing (2) is not used.

Call Processing (3)

Call Processing (3) is not used.

Call Processing (4)

Call Processing (4) is not used.

Call Processing (5)

Call Processing (5) is not used.

Call Processing (6)

Call Processing (6) is not used.

Call Processing (7)

Call Processing (7) is not used.

Call Processing (8)

Table 4-3 lists the details of the Call Processing (8) warning event. To monitor and correct the cause of the event, refer to the "No Route Available for Called Number—Call Processing (8)" section on page 4-28.

Table 4-3 Call Processing (8) Details

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	The call originated 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 the parameters that need to be corrected. Refer to the office records for the subscriber.
Secondary Cause	Parameter(s) in the subscriber and/or dial-plan table are missing or incorrect for the 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** command.

Call Processing (9)

Table 4-4 lists the details of the Call Processing (9) informational event. For additional information, refer to the "No Route Available for Carrier Dialed—Call Processing (9)" section on page 4-28.

Table 4-4 Call Processing (9) Details

Description	No Route Available for Carrier Dialed
Severity	Information
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 the 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 is not specified or is incorrect in the dial-plan table, enter the correct value. Use the **change carrier** or **change route-grp** command.

Call Processing (10)

Call Processing (10) is not used.

Call Processing (11)

Table 4-5 lists the details of the Call Processing (11) minor alarm. To troubleshoot and correct the cause of the alarm, refer to the "Feature Server One Link Down—Call Processing (11)" section on page 4-36.

Table 4-5 Call Processing (11) Details

Description	Feature Server One Link Down
Severity	Minor
Threshold	100
Throttle	0
Datawords	Interface Name—STRING [65] Interface IP Address—STRING [65]
Primary Cause	The hardware is broken.
Primary Action	Check the link interfaces.

Call Processing (12)

Table 4-6 lists the details of the Call Processing (12) critical alarm. To troubleshoot and correct the cause of the alarm, refer to the "Feature Server Both Links Down—Call Processing (12)" section on page 4-38.

Table 4-6 Call Processing (12) Details

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	The hardware is broken.
Primary Action	Check the link interfaces.

Call Processing (13)

Table 4-7 list the details of the Call Processing (13) informational event. For additional information, refer to the "Network Access Server Create Connection Error—Call Processing (13)" section on page 4-28.

Table 4-7 Call Processing (13) Details

Description	Network Access Server Create Connection Error (NAS CRCX Error)
Severity	Information
Threshold	100
Throttle	0
Primary Cause	A preauthentication failure has occurred.
Primary Action	None

Call Processing (14)

Table 4-8 lists the details of the Call Processing (14) informational event. For additional information, refer to the "Network Access Server Authentication Failure—Call Processing (14)" section on page 4-29.

Table 4-8 Call Processing (14) Details

Description	Network Access Server Authentication Failure (NAS Authentication Failure)
Severity	Information
Threshold	100
Throttle	0
Primary Cause	The authentication, authorization, and accounting (AAA) server denied the request.
Primary Action	Check the calling and called numbers.

Call Processing (15)

Table 4-9 lists the details of the Call Processing (15) informational event. 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 4-29.

Table 4-9 Call Processing (15) Details

Description	Cable Modem Termination System Easily Recognizable Identification Not Found in Media Gateway Table (CMTS ER ID Not Found in MGW Table)
Severity	Information
Threshold	100
Throttle	0
Datawords	MGW-NAME—STRING [80]
Primary Cause	The cable modem termination system (CMTS) easily recognizable (ER) entry was not found in the Media Gateway Table.
Primary Action	Provision the CMTS-ER index in the Media Gateway Table.

Call Processing (16)

Table 4-10 lists the details of the Call Processing (16) warning event. 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 4-29.

Table 4-10 Call Processing (16) Details

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.

Call Processing (17)

Table 4-11 lists the details of the Call Processing (17) warning event. To monitor and correct the cause of the event, refer to the "Invalid Route Index Used—Call Processing (17)" section on page 4-29.

Table 4-11 Call Processing (17) Details

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.

Call Processing (18)

Table 4-12 lists the details of the Call Processing (18) warning event. To monitor and correct the cause of the event, refer to the "Unable to Play Announcement—Call Processing (18)" section on page 4-29.

Table 4-12 Call Processing (18) Details

Description	Unable to Play Announcement
Severity	Warning
Threshold	100
Throttle	0
Datawords	Announcement Index—FOUR_BYTES
Primary Cause	An announcement was not provisioned correctly.
Primary Action	Provision the announcement.

Call Processing (19)

Table 4-13 lists the details of the Call Processing (19) warning event. To monitor and correct the cause of the event, refer to the "Call Routed to Unprovisioned Subscriber—Call Processing (19)" section on page 4-29.

Table 4-13 Call Processing (19) Details

Description	Call Routed to Unprovisioned Subscriber
Severity	Warning
Threshold	100
Throttle	0
Datawords	Subscriber Index—FOUR_BYTES Directory Number Dialed—STRING [20]
Primary Cause	A subscriber was not provisioned correctly.
Primary Action	Provision the subscriber.

Call Processing (20)

Table 4-14 lists the details of the Call Processing (20) warning event. 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 4-30.

Table 4-14 Call Processing (20) Details

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	A Trunk Group was not provisioned correctly in the route.
Primary Action	Verify the route and trunk group provisioning.

Call Processing (21)

Table 4-15 lists the details of the Call Processing (21) warning event. To monitor and correct the cause of the event, refer to the "Call Released Due to Maximum Hop Count Exceeded—Call Processing (21)" section on page 4-30.

Table 4-15 Call Processing (21) Details

Description	Call Released Due to Maximum Hop Count Exceeded
Severity	Warning
Threshold	100
Throttle	0
Datawords	Calling Number—STRING [20] Called Number—STRING [20] Hop Count—FOUR_BYTES
Primary Cause	The number of hops between destinations is excessive.
Primary Action	Reduce number of hops between destinations.

Call Processing (22)

Table 4-16 lists the details of the Call Processing (22) warning event. To monitor and correct the cause of the event, refer to the "Trunk Group Index Read Failure—Call Processing (22)" section on page 4-30.

Table 4-16 Call Processing (22) Details

Description	Trunk Group Index Read Failure
Severity	Warning
Threshold	100
Throttle	0
Datawords	Trunk Group Index—FOUR_BYTES Call Index—FOUR_BYTES
Primary Cause	The Trunk Group Index could not be retrieved from call data.
Primary Action	Check the provisioning.

Call Processing (23)

Table 4-17 lists the details of the Call Processing (23) warning event. 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 4-30.

Table 4-17 Call Processing (23) Details

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	The destination termination is not provisioned as a subscriber.
Primary Action	Check the provisioning.

Call Processing (24)

Table 4-18 lists the details of the Call Processing (24) warning event. To monitor and correct the cause of the event, refer to the "Invalid Route for Subscriber Index—Call Processing (24)" section on page 4-30.

Table 4-18 Call Processing (24) Details

Description	Invalid Route for Subscriber Index
Severity	Warning
Threshold	100
Throttle	0
Datawords	Route—STRING [20] Subscriber Index—FOUR_BYTES
Primary Cause	The route is not provisioned correctly for the specified subscriber.
Primary Action	Check the provisioning.

Call Processing (25)

Table 4-19 lists the details of the Call Processing (25) warning event. To monitor and correct the cause of the event, refer to the "Invalid Route Group for Subscriber Routing—Call Processing (25)" section on page 4-30.

Table 4-19 Call Processing (25) Details

Description	Invalid Route Group for Subscriber Routing
Severity	Warning
Threshold	100
Throttle	0
Datawords	Route—STRING [20] Subscriber Index—FOUR_BYTES
Primary Cause	The route group is not provisioned correctly for the specified subscriber.
Primary Action	Check the provisioning.

Call Processing (26)

Table 4-20 lists the details of the Call Processing (26) warning event. To monitor and correct the cause of the event, refer to the "Invalid Trunk Group for Subscriber Routing—Call Processing (26)" section on page 4-31.

Table 4-20 Call Processing (26) Details

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	The trunk group is not provisioned correctly for the specified subscriber.
Primary Action	Check the provisioning.

Call Processing (27)

Table 4-21 lists the details of the Call Processing (27) warning event. 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 4-31.

Table 4-21 Call Processing (27) Details

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	The subscriber provisioning is not in the correct state.
Primary Action	Check the provisioning.

Call Processing (28)

Table 4-22 lists the details of the Call Processing (28) warning event. To monitor and correct the cause of the event, refer to the "Route Name Does Not Exist—Call Processing (28)" section on page 4-31.

Table 4-22 Call Processing (28) Details

Description	Route Name Does Not Exist
Severity	Warning
Threshold	100
Throttle	0
Datawords	Route Name—STRING [40]
Primary Cause	The route is not correctly provisioned.
Primary Action	Check the provisioning.

Call Processing (29)

Table 4-23 lists the details of the Call Processing (29) warning event. To monitor and correct the cause of the event, refer to the "Routing Selection Failure—Call Processing (29)" section on page 4-31.

Table 4-23 Call Processing (29) Details

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	The route is not correctly provisioned.
Primary Action	Check the provisioning.

Call Processing (30)

Table 4-24 lists the details of the Call Processing (30) warning event. To monitor and correct the cause of the event, refer to the "Customer-Originated Trace Test Failed—Call Processing (30)" section on page 4-31.

Table 4-24 Call Processing (30) Details

Description	Customer-Originated Trace Test Failed (COT Test Failed)
Severity	Warning
Threshold	100
Throttle	0
Datawords	Termination Index—FOUR_BYTES
Primary Cause	A customer-originated trace (COT) test has failed.
Primary Action	Contact the Cisco Technical Assistance Center (TAC) for information on how to further debug the problem.

Call Processing (31)

Table 4-25 lists the details of the Call Processing (31) warning event. To monitor and correct the cause of the event, refer to the "Call Authorization Failure—Call Processing (31)" section on page 4-31.

Table 4-25 Call Processing (31) Details

Description	Call Authorization Failure
Severity	Warning
Threshold	100
Throttle	0
Datawords	Calling Number—STRING [20] Called Number—STRING [20]
Primary Cause	Due to incorrect provisioning the call cannot be completed.
Primary Action	Contact Cisco TAC for more information.

Call Processing (32)

Table 4-26 lists the details of the Call Processing (32) warning event. To monitor and correct the cause of the event, refer to the "Country Code Dialing Plan Error—Call Processing (32)" section on page 4-31.

Table 4-26 Call Processing (32) Details

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 the provisioning.

Call Processing (33)

Table 4-27 lists the details of the Call Processing (33) warning event. To monitor and correct the cause of the event, refer to the "Invalid Call—Call Processing (33)" section on page 4-32.

Table 4-27 Call Processing (33) Details

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 the provisioning and the number dialed.

Call Processing (34)

Table 4-28 lists the details of the Call Processing (34) warning event. 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 4-32.

Table 4-28 Call Processing (34) Details

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 the provisioning and the number dialed.

Call Processing (35)

Table 4-29 lists the details of the Call Processing (35) warning event. 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 4-32.

Table 4-29 Call Processing (35) Details

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 the provisioning and the number tested.

Call Processing (36)

Table 4-30 lists the details of the Call Processing (36) warning event. To monitor and correct the cause of the event, refer to the "Invalid or Unknown Nature of Address—Call Processing (36)" section on page 4-32.

Table 4-30 Call Processing (36) Details

Description	Invalid or Unknown Nature of Address (Invalid or Unknown NOA)
Severity	Warning
Threshold	100
Throttle	0
Datawords	NOA Received—FOUR_BYTES Calling Number—STRING [20] Called Number—STRING [20]
Primary Cause	The nature of address (NOA) was incorrect in the dial plan.
Primary Action	Check the provisioning.

Call Processing (37)

Table 4-31 lists the details of the Call Processing (37) warning event. To monitor and correct the cause of the event, refer to the "Call Failure—Call Processing (37)" section on page 4-32.

Table 4-31 Call Processing (37) Details

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 reason indicated in the Failure Indication dataword.
Primary Action	Contact Cisco TAC for more information.

Call Processing (38)

Table 4-32 lists the details of the Call Processing (38) minor alarm. 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 4-39.

Table 4-32 Call Processing (38) Details

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.

Call Processing (39)

Table 4-33 lists the details of the Call Processing (39) warning event. 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 4-33.

Table 4-33 Call Processing (39) Details

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	The initial address message (IAM) for test call was blocked due to congestion or isolation.
Primary Action	Correct the congestion or isolation problem and place the test call again from a remote system.

Call Processing (40)

Table 4-34 lists the details of the Call Processing (40) warning event. 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 4-33.

Table 4-34 Call Processing (40) Details

Description	Interactive Voice Response Real Time Transport Protocol Session Fail (IVR RTP 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 trunk group index are provided if known at the time the event report is issued.

Call Processing (41)

Table 4-35 lists the details of the Call Processing (41) minor alarm. To troubleshoot and correct the cause of the alarm, refer to the "Invite Message From Unauthorized Call Agent—Call Processing (41)" section on page 4-39.

Table 4-35 Call Processing (41) Details

Description	Invite Message From Unauthorized Call Agent (Invite Message From Unauthorized CA)
Severity	Minor
Threshold	100
Throttle	0
Datawords	Unauthorized Call Agent DN—STRING [128] Platform Name—STRING [32]
Primary Cause	The call-agent table is not configured properly.
Primary Action	Reconfigure the call-agent table to have the authorized call agent (CA).
Secondary Cause	A potential intrusion has occurred if the network-ID is mismatched from the local network.
Secondary Action	Configure the network to block the unauthorized network-ID.

Call Processing (42)

Table 4-36 lists the details of the Call Processing (42) informational event. For additional information, refer to "Call Failed After Local Number Portability Query With Location Routing Number of This Cisco BTS 10200 and the Directory Number—Call Processing (42)" section on page 4-33.

Table 4-36 Call Processing (42) Details

Description	Call Failed After Local Number Portability Query with Location Routing Number of This Cisco BTS 10200 and the Directory Number (Call Failed after LNP Query with LRN of this switch and the DN)
Severity	Information
Threshold	100
Throttle	0
Datawords	Calling Number—STRING [20] Called Number (GAP)—STRING [20] Location Routing Number (LRN)—STRING [20] Jurisdiction Information Parameter—STRING [20]
Primary Cause	The provisioning of the ported-in subscriber has not been completed.
Primary Action	Find out if the given DN has been provisioned correctly in the reporting Cisco BTS 10200. If there is an error in the LNP database (SCP) or other switch, then notify the appropriate administrators. Note that porting of the subscriber and DN from the donor switch to the recipient switch, and the associated updates of the Location Routing Number (LRN) in all the SCP databases, might not occur at exactly the same time. Therefore it must be expected that some call failures might occur until the porting process has completed at all network nodes. Once the porting process is completed, if mis-routing still occurs, then the listed actions should be taken to resolve the issue.
Secondary Cause	The LNP database (SCP) has an incorrect location routing number (LRN) for the given directory number (DN).

Call Processing (43)

Table 4-37 lists the details of the Call Processing (43) warning event. To monitor and correct the cause of the event, refer to the "Call Processing Session Initiation Protocol Trigger Provisioning Error—Call Processing (43)" section on page 4-33.

Table 4-37 Call Processing (43) Details

Description	Call Processing Session Initiation Protocol Trigger Provisioning Error (Call Processing SIP Trigger Provisioning Error)
Severity	Warning
Threshold	100
Throttle	0
Datawords	Calling Party Number—STRING [64] Called Party Number—STRING [64] Call ID- FOUR_BYTES OBCSM/TBCSM SIP Trigger—STRING [8]
Primary Cause	A provisioning data discrepancy between the Application Server (AS) and the Cisco BTS 10200 has occurred.
Primary Action	Modify the provisioning data either in the Cisco BTS 10200 or the AS.

Call Processing (44)

Table 4-38 lists the details of the Call Processing (44) warning event. To monitor and correct the cause of the event, refer to the "Call Processing No Session Initiation Protocol Trigger Context Found—Call Processing (44)" section on page 4-34.

Table 4-38 Call Processing (44) Details

Description	Call Processing No Session Initiation Protocol Trigger Context Found (Call Processing No SIP Trig Context Found)
Severity	Warning
Threshold	100
Throttle	0
Datawords	Calling Party Number—STRING [64] Called Party Number—STRING [64] Call ID- FOUR_BYTES Inbound Context String—STRING [64]
Primary Cause	An invalid service_ref in the SIP invite message coming from the AS has occurred.
Primary Action	Report the Cisco BTS 10200 and the AS with the received service_ref string to Cisco TAC.

Call Processing (45)

Table 4-39 lists the details of the Call Processing (45) warning event. To monitor and correct the cause of the event, refer to the "Context In Call From Application Server Not Found—Call Processing (45)" section on page 4-34.

Table 4-39 Call Processing (45) Details

Description	Context In Call From Application Server Not Found (Context in Call from App Server not Found)
Severity	Warning
Threshold	100
Throttle	0
Primary Cause	The Cisco BTS 10200 has received an invite from an AS which contains a context ID in the route header which is invalid. It may be that the AS has not properly returned the route header.
Primary Action	Get the AS to return the Cisco BTS 10200 route header correctly.
Secondary Cause	It is possible that the Cisco BTS 10200 cleared the call and removed the context before the AS returned an invite to the Cisco BTS 10200.
Secondary Action	Check timing for the calls returned to the Cisco BTS 10200 from the AS.

Call Processing (46)

Table 4-40 lists the details of the Call Processing (46) informational event. For additional information, refer to "Limit of Calls Allowed for the Pool Has Been Reached—Call Processing (46)" section on page 4-34.

Table 4-40 Call Processing (46) Details

Description	Limit of Calls Allowed for the Pool Has Been Reached
Severity	Information
Threshold	100
Throttle	0
Datawords	Pool ID - STRING [32]
Primary Cause	Number of calls over all SIP trunk groups utilizing the pool exceeds size of the pool.
Primary Action	If situation persists, you may wish to resize the affected pool or you may need to do additional traffic engineering.

Call Processing (47)

Table 4-41 lists the details of the Call Processing (47) warning event. To monitor and correct the cause of the event, refer to the "System Limit of Calls Allowed for Pools Has Been Reached—Call Processing (47)" section on page 4-34.

Table 4-41 Call Processing (47) Details

Description	System Limit of Calls Allowed for Pools Has Been Reached
Severity	Warning
Threshold	100
Throttle	0
Primary Cause	The number of calls over all SIP trunk group pools exceeds the allowable system value.
Primary Action	If the situation persists, additional traffic engineering is needed.

Monitoring Call Processing Events

This section provides the information needed for monitoring and correcting call processing events. Table 4-42 lists all of the call processing events in numerical order and provides cross-references to each subsection.

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

Table 4-42 Cisco BTS 10200 Call Processing Events

Event Type	Event Name	Event Severity
Call Processing (1)	Test Report—Call Processing (1)	Information
Call Processing (8)	No Route Available for Called Number—Call Processing (8)	Warning
Call Processing (9)	No Route Available for Carrier Dialed—Call Processing (9)	Information
Call Processing (11)	Feature Server One Link Down—Call Processing (11)	Minor
Call Processing (12)	Feature Server Both Links Down—Call Processing (12)	Critical
Call Processing (13)	Network Access Server Create Connection Error—Call Processing (13)	Information
Call Processing (14)	Network Access Server Authentication Failure—Call Processing (14)	Information
Call Processing (15)	Cable Modem Termination System Easily Recognizable Identification Not Found in Media Gateway Table—Call Processing (15)	Information
Call Processing (16)	Route Index Has No Trunk Group Assigned—Call Processing (16)	Warning
Call Processing (17)	Invalid Route Index Used—Call Processing (17)	Warning
Call Processing (18)	Unable to Play Announcement—Call Processing (18)	Warning
Call Processing (19)	Call Routed to Unprovisioned Subscriber—Call Processing (19)	Warning
Call Processing (20)	No Route or Trunk Group Available to Route Call—Call Processing (20)	Warning
Call Processing (21)	Call Released Due to Maximum Hop Count Exceeded—Call Processing (21)	Warning
Call Processing (22)	Trunk Group Index Read Failure—Call Processing (22)	Warning
Call Processing (23)	Routing Error: Termination Is Not a Subscriber—Call Processing (23)	Warning
Call Processing (24)	Invalid Route for Subscriber Index—Call Processing (24)	Warning
Call Processing (25)	Invalid Route Group for Subscriber Routing—Call Processing (25)	Warning
Call Processing (26)	Invalid Trunk Group for Subscriber Routing—Call Processing (26)	Warning

Table 4-42 Cisco BTS 10200 Call Processing Events (continued)

Event Type	Event Name	Event Severity
Call Processing (27)	Unable to Route: Blocked by Destination Subscriber Status—Call Processing (27)	Warning
Call Processing (28)	Route Name Does Not Exist—Call Processing (28)	Warning
Call Processing (29)	Routing Selection Failure—Call Processing (29)	Warning
Call Processing (30)	Customer-Originated Trace Test Failed—Call Processing (30)	Warning
Call Processing (31)	Call Authorization Failure—Call Processing (31)	Warning
Call Processing (32)	Country Code Dialing Plan Error—Call Processing (32)	Warning
Call Processing (33)	Invalid Call—Call Processing (33)	Warning
Call Processing (34)	Dial Plan Information Not Found for Digits Received—Call Processing (34)	Warning
Call Processing (35)	Dial Plan Information for Test Call Not Found—Call Processing (35)	Warning
Call Processing (36)	Invalid or Unknown Nature of Address—Call Processing (36)	Warning
Call Processing (37)	Call Failure—Call Processing (37)	Warning
Call Processing (38)	Release Cause 25 Exchange Routing Error Received—Call Processing (38)	Minor
Call Processing (39)	Test Call Blocked Due to Congestion or Isolation—Call Processing (39)	Warning
Call Processing (40)	Interactive Voice Response Real Time Transport Protocol Session Fail—Call Processing (40)	Warning
Call Processing (41)	Invite Message From Unauthorized Call Agent—Call Processing (41)	Minor
Call Processing (42)	Call Failed After Local Number Portability Query With Location Routing Number of This Cisco BTS 10200 and the Directory Number—Call Processing (42)	Information
Call Processing (43)	Call Processing Session Initiation Protocol Trigger Provisioning Error—Call Processing (43)	Warning
Call Processing (44)	Call Processing No Session Initiation Protocol Trigger Context Found—Call Processing (44)	Warning
Call Processing (45)	Context In Call From Application Server Not Found—Call Processing (45)	Warning
Call Processing (46)	Limit of Calls Allowed for the Pool Has Been Reached—Call Processing (46)	Information
Call Processing (47)	System Limit of Calls Allowed for Pools Has Been Reached—Call Processing (47)	Warning

Test Report—Call Processing (1)

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

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

The No Route Available for Called Number event functions as a warning that no route is 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 (1 byte), Orig Sub or trunk group (TG) ID (8 bytes), calling party number (20), and called party number (20) data words in the event report indicate the 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 and a PIC is used, 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** command.

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

The No Route Available for Carrier Dialed event functions as a warning that no route is available for the dialed carrier. The primary cause for the event is that no route is available for the IXC dialed. The Orig Type (1 byte), Orig Sub or TG ID (8 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 is not specified or is incorrect in the dial-plan table, enter the correct value. 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 4-36.

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 4-38.

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) preauthentication 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 call 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 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, if necessary, correct the provisioning of the announcement.

Call Routed to Unprovisioned Subscriber—Call Processing (19)

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

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

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

Call Released Due to Maximum Hop Count Exceeded—Call Processing (21)

The Call Released Due to Maximum Hop Count Exceeded event functions as a warning that the call was released due to the maximum hop count 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 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 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 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 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 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 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 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 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 failed. To correct the primary cause of the event, contact Cisco TAC for information on how to debug the problem.

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 that a provisioning error is not allowing the call to be completed. To correct the primary cause of the event, contact Cisco TAC.

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 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 provisioning. Additionally, check the number dialed to verify that it is a valid number.

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 dial plan provisioning. Additionally, check the number dialed to verify that it is a valid number.

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 dial plan provisioning. Additionally, check the number tested to verify that it is a valid number.

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 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 (4 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.

Prior to contacting Cisco TAC, collect a billing-record for the failed call using the following:

```
report billing-record orignumber=<string>
```

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 4-39.

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 in the network. The primary cause of the event is that the IAM for test call was blocked due to congestion or isolation. To correct the primary cause of the event, correct the 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 4-39.

Call Failed After Local Number Portability Query With Location Routing Number of This Cisco BTS 10200 and the Directory Number—Call Processing (42)

The Call Failed after Local Number Portability Query With Location Routing Number of This Cisco BTS 10200 and the Directory Number event serves as an information alert that the provisioning of a ported-in subscriber has not been completed. To correct the primary cause of the event, verify whether the given DN has been provisioned correctly in the reporting Cisco BTS 10200. If there is an error in the LNP database (SCP) or in another switch, notify the appropriate administrators. Note that porting of the subscriber and DN from the donor switch to the recipient switch, and associated updates of the Location Routing Number (LRN) in all the SCP databases, might not all occur at exactly the same time. Therefore it must be expected that some call failures might occur until the porting process has completed at all network nodes. If you think the porting process is complete but mis-routing still occurs, take the above actions to resolve the issue. The secondary cause of the event is that the LNP database (SCP) has an incorrect LRN for the given DN.

Call Processing Session Initiation Protocol Trigger Provisioning Error—Call Processing (43)

The Call Processing Session Initiation Protocol Trigger Provisioning Error event serves as warning that a provisioning data discrepancy between the Application Server and the Cisco BTS 10200 has occurred. To correct the cause of the event, modify the provisioning data either in the Cisco BTS 10200 or the Application Server.

Call Processing No Session Initiation Protocol Trigger Context Found—Call Processing (44)

The Call Processing No Session Initiation Protocol Trigger Context Found event serves as a warning that there is an invalid "service_ref" string in the SIP INVITE message coming from the Application Server. To correct the cause of the event, report the Cisco BTS 10200 and the Application Server with the received “service_ref” string to Cisco TAC.

Context In Call From Application Server Not Found—Call Processing (45)

The Context In Call From Application Server Not Found event serves as a warning that a Cisco BTS 10200 has received an invite from an application server which contains a context ID in the route header which is invalid. It may be that the Application Server has not properly returned the route header. Additionally, it is possible that the Cisco BTS 10200 has cleared the call and removed the context before the application server returned an invite message to the Cisco BTS 10200. To correct the cause of the event, get the application server to correctly return the Cisco BTS 10200 route header back to the Cisco BTS 10200 and check timing for the calls returned to the Cisco BTS 10200 from the application server.

Limit of Calls Allowed for the Pool Has Been Reached—Call Processing (46)

The Limit of Calls Allowed for the Pool Has Been Reached event serves as an information alert that the number of calls over all SIP trunk groups utilizing the pool exceeds size of the pool. If the situation persists, you may wish to resize the affected pool or you may wish to do additional traffic engineering.

System Limit of Calls Allowed for Pools Has Been Reached—Call Processing (47)

The System Limit of Calls Allowed for Pools Has Been Reached event serves as a warning that the number of calls over all SIP trunk group pools exceeds allowable system value. If the situation persists, additional traffic engineering is needed.

Troubleshooting Call Processing Alarms

This section provides the information you need to monitor and correct call processing alarms. Table 4-43 lists all of the call processing alarms in numerical order and provides cross-references to each subsection.

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

Table 4-43 Cisco BTS 10200 Call Processing Alarms

Alarm Type	Alarm Name	Alarm Severity
Call Processing (11)	Feature Server One Link Down—Call Processing (11)	Minor
Call Processing (12)	Feature Server Both Links Down—Call Processing (12)	Critical
Call Processing (38)	Release Cause 25 Exchange Routing Error Received—Call Processing (38)	Minor
Call Processing (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/docs/ios/12_2/interface/command/reference/irfshoin.html

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/docs/ios/12_2/interface/command/reference/irfshoin.html

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 4-31 for additional troubleshooting information.

Invite Message From Unauthorized Call Agent—Call Processing (41)

The Invite Message From Unauthorized Call Agent alarm (minor) indicates that an 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: August 10, 2011, OL-25016-01

Introduction

This chapter provides the information needed for monitoring and troubleshooting 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 for monitoring and correcting the configuration events.
- Troubleshooting Configuration Alarms—Provides the information needed for troubleshooting and correcting the configuration alarms.

Configuration Events and Alarms

This section provides a brief overview of the configuration events and alarms for the Cisco BTS 10200 Softswitch; the event and alarms are arranged in numerical order. Table 5-1 lists all of the configuration events and alarms by severity.

Note Refer to the "Obtaining Documentation and Submitting a Service Request" section on page 1 for detailed instructions on contacting Cisco TAC and opening a service request.

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	Information	Not Used
Configuration (4)	Configuration (3)	Configuration (5)	Configuration (6)	Configuration (1)	
			Configuration (7)	Configuration (2)	
			Configuration (8)		

Configuration (1)

Table 5-2 lists the details of the Configuration (1) informational event. For additional information, refer to the "Test Report—Configuration (1)" section on page 5-6.

Table 5-2 Configuration (1) Details

Description	Test Report
Severity	Information
Threshold	10000
Throttle	0

Configuration (2)

Table 5-3 lists the details of the Configuration (2) informational event. For additional information, refer to the "Signaling Media Gateway Adapter Wrongly Configured Domain Name—Configuration (2)" section on page 5-6.

Table 5-3 Configuration (2) Details

Description	Signaling Media Gateway Adapter Wrongly Configured Domain Name (Signaling MGA Wrongly Configured Domain Name)
Severity	Information
Threshold	1
Throttle	1
Datawords	Configured Domain Na—STRING [256] Cause—STRING [128]
Primary Cause	The domain name is invalid.
Primary Action	Check the domain name system (DNS) server and correct the domain name.
Secondary Cause	At least half of the local machine address does not match the Media Gateway Control Protocol (MGCP) domain name.
Secondary Action	Check the DNS server for the domain name to ensure that the Internet Protocol (IP) address is correct.

Configuration (3)

Table 5-4 lists the details of the Configuration (3) major alarm. To troubleshoot and correct the cause of the alarm, refer to the "Mate Configuration Error—Configuration (3)" section on page 5-8.

Table 5-4 Configuration (3) Details

Description	Keep Alive Module: Mate Configuration Error (KAM: Mate Configuration Error)
Severity	Major
Threshold	100
Throttle	0
Datawords	Reason—STRING [80]
Primary Cause	The mate and the local are configured as the same side.
Primary Action	Configure one side of the platform to come up opposite of its mate.
Secondary Cause	The mate is configured with wrong mate red DNS name.
Secondary Action	Configure the mate DNS name properly for mate.
Ternary Cause	Mate read and DNS entries are changed.

Configuration (4)

Table 5-5 lists the details of the Configuration (4) critical alarm. To troubleshoot and correct the cause of the alarm, refer to the "Configuration Error—Configuration (4)" section on page 5-8.

Table 5-5 Configuration (4) Details

Description	Configuration Error
Severity	Critical
Threshold	100
Throttle	0
Datawords	Reason—STRING [80]
Primary Cause	The wrong configuration is in the platform.cfg file.
Primary Action	Correct the appropriate parameters in the platform.cfg file.

Configuration (5)

Table 5-6 lists the details of the Configuration (5) minor alarm. 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 5-8.

Table 5-6 Configuration (5) Details

Description	Feature Server Database and Command Line Host Mismatch (Feature—Server DB 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 and –port.

Configuration (6)

Table 5-7 lists the details of the Configuration (6) warning event. To monitor and correct the cause of the event, refer to the "FIMXML Parse Error—Configuration (6)" section on page 5-7.

Table 5-7 Configuration (6) Details

Description	FIMXML Parse Error (Flexible Feature Interaction Manager Through Extensible Markup Language Parse Error)
Severity	Warning
Threshold	100
Throttle	0
Primary Cause	The Cisco BTS 10200 software is released with a file named FIMXMLRules.xml. This file is only read during system initialization. It defines how to handle certain features provided on an external application server. The file might be missing.
Primary Action	Install the FIMXMLRules.xml file in the appropriate directory.
Secondary Cause	The FIMXMLRules.xml file has been incorrectly modified.
Secondary Action	Install a valid FIMXML file.

Configuration (7)

Table 5-8 lists the details of the Configuration (7) warning event. To monitor and correct the cause of the event, refer to the "Application Server Provisioning Error—Configuration (7)" section on page 5-7.

Table 5-8 Configuration (7) Details

Description	Application Server Provisioning Error
Severity	Warning
Threshold	100
Throttle	0
Primary Cause	The external application server has returned a SIP response code that indicates a subscriber is not provisioned on the AS.
Primary Action	Provision the application server to handle all subscribers which are provisioned on the Cisco BTS 10200 to use the applications on that server.

Configuration (8)

Table 5-9 lists the details of the Configuration (8) warning event. To monitor and correct the cause of the event, refer to the "Cisco BTS 10200 Provisioning for External Applications Is Not Complete—Configuration (8)" section on page 5-7.

Table 5-9 Configuration (8) Details

Description	Cisco BTS 10200 Provisioning for External Applications is Not Complete
Severity	Warning
Threshold	100
Throttle	0
Primary Cause	The Cisco BTS 10200 call agent is provisioned to send a trigger to the feature server for the offhook delay trigger (OHD) feature or the terminating attempt trigger (TAT) feature. The subscriber is not provisioned to define the sip-trigger-profile ID.
Primary Action	Provision the sip-trigger-profile ID for each subscriber that has OHD or TAT provisioned.

Monitoring Configuration Events

This section provides the information you need for monitoring and correcting configuration events. Table 5-10 lists all of the configuration events in numerical order and provides cross-references to each subsection.

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

Table 5-10 Cisco BTS 10200 Configuration Events

Event Type	Event Name	Event Severity
Configuration (1)	Test Report—Configuration (1)	Information
Configuration (2)	Signaling Media Gateway Adapter Wrongly Configured Domain Name—Configuration (2)	Information
Configuration (3)	Mate Configuration Error—Configuration (3)	Major
Configuration (4)	Configuration Error—Configuration (4)	Critical
Configuration (5)	Feature Server Database and Command Line Host Mismatch—Configuration (5)	Minor
Configuration (6)	FIMXML Parse Error—Configuration (6)	Warning
Configuration (7)	Application Server Provisioning Error—Configuration (7)	Warning
Configuration (8)	Cisco BTS 10200 Provisioning for External Applications Is Not Complete—Configuration (8)	Warning

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 the 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 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 5-8.

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 5-8.

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 5-8.

FIMXML Parse Error—Configuration (6)

The FIMXML Parse Error event serves as warning that the FIMXMLRules.xml file is missing or has been incorrectly modified. The Cisco BTS 10200 software is released with a file named FIMXMLRules.xml. This file is only read during system initialization. It defines how to handle certain features provided on an external application server. The file might be missing, or it might have been incorrectly modified. To correct the primary cause of the FIMXML Parse Error event, install the FIMXMLRules.xml file in the appropriate directory. A secondary cause of the event is that an invalid FIMXMLRules.xml file is installed. To correct the secondary cause of the event, install a valid FIMXMLRules.xml file.

Application Server Provisioning Error—Configuration (7)

The Application Server Provisioning Error event serves as a warning that the external application server has returned a SIP response code that indicates a subscriber is not provisioned on the AS. To correct the cause of the Application Server Provisioning Error event, provision the application server to handle all subscribers who are provisioned on the Cisco BTS 10200 to use applications on that server.

Cisco BTS 10200 Provisioning for External Applications Is Not Complete—Configuration (8)

The Cisco BTS 10200 Provisioning for External Applications Is Not Complete event serves as warning that the Cisco BTS 10200 call agent is provisioned to send a trigger to the Feature Server for OHD or TAT feature. The subscriber is not provisioned to define the sip-trigger-profile ID. To correct the cause of the Cisco BTS 10200 Provisioning for External Applications is not Complete event, provision the sip-trigger-profile ID for each subscriber who has OHD or TAT provisioned.

Troubleshooting Configuration Alarms

This section provides the information needed to monitor and correct configuration alarms. Table 5-11 lists all of the configuration alarms in numerical order and provides cross-references to each subsection.

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

Table 5-11 Cisco BTS 10200 Configuration Alarms

Alarm Type	Alarm Name	Alarm Severity
Configuration (3)	Mate Configuration Error—Configuration (3)	Major
Configuration (4)	Configuration Error—Configuration (4)	Critical
Configuration (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 the alarm is that the mate side and the local side are configured to be 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, check and, if necessary, correct the 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 to match command line –host and –port.

CHAPTER 6

Database Troubleshooting

Revised: August 10, 2011, OL-25016-01

Introduction

This chapter provides the information needed for monitoring and troubleshooting 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 for monitoring and correcting the database events
- Troubleshooting Database Alarms—Provides the information needed for troubleshooting and correcting the database alarms

Database Events and Alarms

This section provides a brief overview of the database events and alarms for the Cisco BTS 10200 Softswitch; the event and alarms are arranged in numerical order. Table 6-1 lists all of the database events and alarms by severity.

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

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	Information	Not Used
Database (3)	Database (6)	Database (7)	Database (2)	Database (1)	
Database (4)	Database (8)	Database (14)	Database (11)	Database (19)	
Database (5)	Database (10)	Database (21)	Database (18)		
Database (9)	Database (13)	Database (23)			
Database (12)	Database (15)				
Database (16)	Database (17)				
	Database (20)				
	Database (22)				
	Database (24)				
	Database (25)				
	Database (26)				
	Database (27)				

Database (1)

Table 6-2 lists the details of the Database (1) informational event. For additional information, refer to the "Test Report—Database (1)" section on page 6-24.

Table 6-2 Database (1) Details

Description	Test Report
Severity	Information
Threshold	10000
Throttle	0

Database (2)

Table 6-3 lists the details of the Database (2) warning event. 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 6-24.

Table 6-3 Database (2) Details

Description	Database Management Update Failure: Master/Slave Database Out of Sync (DBM 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) failed to complete.
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)

Table 6-4 lists the details of the Database (3) critical alarm. 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 6-31.

Table 6-4 Database (3) Details

Description	There Are Errors in Element Management System Database DefError Queue; Contact Database Administrator (There are Errors in EMS Database DefError Queue; Contact DBA)
Severity	Critical
Threshold	100
Throttle	0
Datawords	Host Name—STRING [30] Database Name—STRING [10] Error Count—ONE_BYTE Time Stamp—STRING [20]
Primary Cause	Replication data conflicts have occurred.
Primary Action	The replication data conflicts may require a manual update on the database tables. Contact the Cisco Technical Assistance Center (TAC).
Secondary Cause	An update or delete attempt on nonexisting data has occurred.
Ternary Cause	The unique constraint (primary key) has been violated.

Database (4)

Table 6-5 lists the details of the Database (4) critical alarm. 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 6-32.

Table 6-5 Database (4) Details

Description	Element Management System Database HeartBeat: Replication Push Job Broken (EMS DB_Heart_Beat: Replication Push Job Broken)
Severity	Critical
Threshold	100
Throttle	0
Datawords	Host Name—STRING [30] Local Database—STRING [10] Remote Database—STRING [10] Job—STRING [5] Time Stamp—STRING [20]
Primary Cause	The remote database is not accessible.
Primary Action	Restart or restore the remote database.
Secondary Cause	The remote database is down.
Secondary Action	Restart the remote listener process.
Ternary Cause	The remote Oracle listener process has died.
Ternary Action	Correct the network connection problem.
Subsequent Cause	The network connection is broken.

Database (5)

Table 6-6 lists the details of the Database (5) critical alarm. To troubleshoot and correct the cause of the alarm, refer to the "Element Management System Database HeartBeat Process Died—Database (5)" section on page 6-32.

Table 6-6 Database (5) Details

Description	Element Management System Database HeartBeat Process Died (EMS DBHeartBeat Process Died)
Severity	Critical
Threshold	100
Throttle	0
Datawords	Host Name—STRING [30] Database Name—STRING [10] Time Stamp—STRING [20]
Primary Cause	The DBHeartBeat process has been terminated by the system manager program (SMG) or stopped by the platform.
Primary Action	Restart the DBHeartBeat process by entering the **dbinit -H -i start** command as an Oracle user, or by entering the **platform start** command as a root user.

Database (6)

Table 6-7 lists the details of the Database (6) major alarm. 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 6-33.

Table 6-7 Database (6) Details

Description	Element Management System Database Replication DefTranDest Queue Overloaded (EMS Database Replication DefTranDest Queue Overloaded)
Severity	Major
Threshold	100
Throttle	0
Datawords	Host Name—STRING [30] Database Name—STRING [10] Threshold—FOUR_BYTES Time Stamp—STRING [20]
Primary Cause	The replication push job is broken.
Primary Action	Correct problems on the remote database.
Secondary Cause	The remote database is not accessible.
Secondary Action	Make sure that the DBHeartBeat process is up.
Ternary Cause	The database is overloaded.
Ternary Action	Troubleshoot the database performance.

Database (7)

Table 6-8 lists the details of the Database (7) minor alarm. 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 6-34.

Table 6-8 Database (7) Details

Description	Element Management System Database DefTran Queue is Overloaded (EMS Database DefTran Queue is Overloaded)
Severity	Minor
Threshold	100
Throttle	0
Datawords	Host Name—STRING [30] Database Name—STRING [10] Threshold—TWO_BYTES Time Stamp—STRING [20]
Primary Cause	The replication DefTranDest queue is overloaded.
Primary Action	Resume the replication activities.
Secondary Cause	There are too many errors in the DefError queue.
Secondary Action	Correct the replication errors.
Ternary Cause	The replication purge job is broken or overloaded.
Ternary Action	Enable the replication purge job.

Database (8)

Table 6-9 lists the details of the Database (8) major alarm. 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 6-34.

Table 6-9 Database (8) Details

Description	Element Management System Database Tablespace is Out of Free Space (EMS Database Tablespace is Out of Free Space)
Severity	Major
Threshold	100
Throttle	0
Datawords	Host Name—STRING [30] Database Name—STRING [10] Tablespace Name—STRING [30] Total Free Space—TWO_BYTES Time Stamp—STRING [20]
Primary Cause	An increase data volume or transactions has occurred.
Primary Action	Add more space to the tablespace.

Database (9)

Table 6-10 lists the details of the Database (9) critical alarm. 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 6-35.

Table 6-10 Database (9) Details

Description	Urgent: Element Management System Database Archive Log Directory is Getting Full (Urgent: EMS Database Archive Log Directory is Getting Full)
Severity	Critical
Threshold	100
Throttle	0
Datawords	Host Name—STRING [30] Database Name—STRING [10] Directory Name—STRING [100] Free Space—TWO_BYTES Time Stamp—STRING [20]
Primary Cause	The transaction volume has increased.
Primary Action	Back up and clean up the archive log files.
Secondary Action	Add more space to the archive log directory.

Database (10)

Table 6-11 lists the details of the Database (10) major alarm. To troubleshoot and correct the cause of the alarm, refer to the "Element Management System Database: Back Up Fails—Database (10)" section on page 6-35.

Table 6-11 Database (10) Details

Description	Element Management System Database: Back Up Fails (EMS Database: Back Up 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	The system or hardware is unstable.
Primary Action	Restart back up process.

Database (11)

Table 6-12 lists the details of the Database (11) major alarm. To troubleshoot and correct the cause of the alarm, refer to the "Element Management System Database Alert.log Alerts—Database (11)" section on page 6-35.

Table 6-12 Database (11) Details

Description	Element Management System Database Alert.log Alerts (EMS 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- errors report in alert.log file is documented in the $ORACLE_HOME/rdbms/mesg/oraus.msg file. Log in to the EMS system as an oracle user (or su–oracle) to view this file. If more information is needed, contact Cisco TAC for database support, or query Oracle metalink library at http://metalink.oracle.com.
Primary Action	The corrective action is documented in the $ORACLE_HOME/rdbms/mesg/oraus.msg file. Log in to the EMS system as an oracle user (or su–oracle) to view this file. If more information is needed, contact Cisco TAC for database support, or query Oracle Metalink library at http://metalink.oracle.com. The alert.log file is the global message file for errors issued by all Oracle background processes. The majority of error conditions might require administrator's investigation and manual correction.

Database (12)

Table 6-13 lists the details of the Database (12) critical alarm. To troubleshoot and correct the cause of the alarm, refer to the "Element Management System Database Process Died—Database (12)" section on page 6-35.

Table 6-13 Database (12) Details

Description	Element Management System Database Process Died (EMS 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 the local process is not running. 2. Cannot_connect_database if the local database (DB) is unreachable. 3. Cannot_connect if the remote DB is unreachable.
Primary Action	Restart the process.
Secondary Action	Contact Cisco TAC.

Database (13)

Table 6-14 lists the details of the Database (13) major alarm. To troubleshoot and correct the cause of the alarm, refer to the "Element Management System Database Performance Alert—Database (13)" section on page 6-35.

Table 6-14 Database (13) Details

Description	Element Management System Database Performance Alert (EMS 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 the Stat Event Name dataword.
Primary Action	Contact Cisco TAC.
Secondary Action	Perform a database performance tuning.

Database (14)

Table 6-15 lists the details of the Database (14) minor alarm. To troubleshoot and correct the cause of the alarm, refer to the "Table Size Exceeds Minor Threshold Limit—Database (14)" section on page 6-36.

Table 6-15 Database (14) Details

Description	Table Size Exceeds Minor Threshold Limit
Severity	Minor
Threshold	100
Throttle	0
Datawords	Table Name—STRING [32]
Primary Cause	The preprovisioned size for the stated table is nearing the licensed limit on the number of entries it can hold.
Primary Action	Contact Cisco TAC to purchase additional entry space for this particular table.

Database (15)

Table 6-16 lists the details of the Database (15) major alarm. To troubleshoot and correct the cause of the alarm, refer to the "Table Size Exceeds Major Threshold Limit—Database (15)" section on page 6-36.

Table 6-16 Database (15) Details

Description	Table Size Exceeds Major Threshold Limit
Severity	Major
Threshold	100
Throttle	0
Datawords	Table Name—STRING [32]
Primary Cause	The major threshold limit has been exceeded.
Primary Action	Not applicable.

Database (16)

Table 6-17 lists the details of the Database (16) critical alarm. To troubleshoot and correct the cause of the alarm, refer to the "Table Size Exceeds Critical Threshold Limit—Database (16)" section on page 6-36.

Table 6-17 Database (16) Details

Description	Table Size Exceeds Critical Threshold Limit
Severity	Critical
Threshold	100
Throttle	0
Datawords	Table Name—STRING [32]
Primary Cause	The critical threshold limit has been exceeded.
Primary Action	Not applicable.

Database (17)

Table 6-18 lists the details of the Database (17) major alarm. To troubleshoot and correct the cause of the alarm, refer to the "Data Replication Failed—Database (17)" section on page 6-36.

Table 6-18 Database (17) Details

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	The index size is out of range.
Secondary Cause	Record the index size mismatch.

Database (18)

Table 6-19 lists the details of the Database (18) warning event. To monitor and correct the cause of the event, refer to the "Unexpected Runtime Data Interaction—Database (18)" section on page 6-27.

Table 6-19 Database (18) Details

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	An unexpected data interaction has been detected at the runtime in the call agent or the feature server.
Primary Action	Collect the logs and contact Cisco TAC.

Database (19)

Table 6-20 lists the details of the Database (19) informational event. For additional information, refer to the "Daily Database Back Up Completed Successfully—Database (19)" section on page 6-27.

Table 6-20 Database (19) Details

Description	Daily Database Back Up Completed Successfully
Severity	Information
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	Not applicable.

Database (20)

Table 6-21 lists the details of the Database (20) major alarm. To troubleshoot and correct the cause of the alarm, refer to the "Replication Data Flush Timeout During Switchover—Database (20)" section on page 6-36.

Table 6-21 Database (20) Details

Description	Replication Data Flush Timeout During Switchover
Severity	Major
Threshold	100
Throttle	0
Datawords	Tables Failed—STRING [20]
Primary Cause	An replication module software problem has occurred.
Primary Action	The database restore procedure needs to be executed on the side of the system which goes active after the switchover. Any alarms should be cleared manually after the recovery action is taken.

Database (21)

Table 6-22 lists the details of the Database (21) minor alarm. To troubleshoot and correct the cause of the alarm, refer to the "Database Statistics Collection Exception—Database (21)" section on page 6-36.

Table 6-22 Database (21) Details

Description	Database Statistics Collection Exception (DB 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 dataword 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 the **oerr ora xxxxx** command as an Oracle user.

Database (22)

Table 6-23 lists the details of the Database (22) major alarm. To troubleshoot and correct the cause of the alarm, refer to the "Unprovisioned Language—Database (22)" section on page 6-37.

Table 6-23 Database (22) Details

Description	Unprovisioned Language
Severity	Major
Threshold	100
Throttle	0
Datawords	Language ID—STRING [4]
Primary Cause	The operator has missed provisioning the language for this alarm in the language table on the EMS.
Primary Action	The operator has to provision the missing language and update the LANGUAGE table.

Database (23)

Table 6-24 lists the details of the Database (23) minor alarm. To troubleshoot and correct the cause of the alarm, refer to the "Element Management System Oracle Database—Minor Error—Database (23)" section on page 6-38.

Table 6-24 Database (23) Details

Description	Element Management System Oracle Database—Minor Error (EMS Oracle Database (ORA)—Minor Error)
Severity	Minor
Threshold	100
Throttle	0
Datawords	HostName—STRING [30] DatabaseName—STRING [10] Message1—STRING [200] Message2—STRING [200] TimeStamp—STRING [20]
Primary Cause	This ORA error is issued by an Oracle background process. The probable cause of the ORA- errors is documented in the $ORACLE_HOME/rdbms/mesg/oraus.msg file. To view the file, log in to the EMS system as root, then su–oracle. If more information is needed, contact Cisco TAC for database support, or query the 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, log in to the EMS system as root, then su–oracle. If more information is needed, contact Cisco TAC for database support, or query the Oracle Metalink library at http://metalink.oracle.com. Many ORA- errors may need an administrator to investigate and resolve the problem. When the problem is resolved, this alarm should be manually cleared by the operator.

Database (24)

Table 6-25 lists the detail of the Database (24) major alarm. To troubleshoot and correct the cause of the alarm, refer to the "Element Management System Oracle Database—Major Error—Database (24)" section on page 6-39.

Table 6-25 Database (24) Details

Description	Element Management System Oracle Database—Major Error (EMS Oracle Database (ORA)—Major Error)
Severity	Major
Threshold	100
Throttle	0
Datawords	HostName—STRING [30] DatabaseName—STRING [10] Message1—STRING [200] Message2—STRING [200] TimeStamp—STRING [20]
Primary Cause	This ORA error is issued by an Oracle background process. The probable cause of the ORA- errors is documented in the $ORACLE_HOME/rdbms/mesg/oraus.msg file. To view the file, log in to the EMS system as root, then su–oracle. If more information is needed, contact Cisco TAC for database support, or query the 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, log in to the EMS system as root, then su–oracle. If more information is needed, contact Cisco TAC for database support, or query the Oracle Metalink library at http://metalink.oracle.com. Many ORA- errors may need an administrator to investigate and resolve the problem. When the problem is resolved, this alarm should be manually cleared by the operator.

Database (25)

Table 6-26 lists the details of the Database (25) major alarm. To troubleshoot and correct the cause of the alarm, refer to the "Secure File Transfer Protocol Transfer Failed—Database (25)" section on page 6-39.

Table 6-26 Database (25) Details

Description	Secure File Transfer Protocol Transfer Failed (SFTP 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 log in to remote host.
Secondary Action	Verify that secure shell (SSH) keys have been preconfigured 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)

Table 6-27 lists the details of the Database (26) major alarm. To troubleshoot and correct the cause of the alarm, refer to the "File Write Error—Database (26)" section on page 6-39.

Table 6-27 Database (26) Details

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	Contact Cisco TAC.

Database (27)

Table 6-28 list the details of the Database (27) major alarm. To troubleshoot and correct the cause of the alarm, refer to the "Failure Setting the Index Table Soft Limit—Database (27)" section on page 39.

Table 6-28 Database (27) Details

Description	Failure Setting the Index Table Soft Limit (Failure Setting the IDX Table Soft Limit)
Severity	Major
Threshold	100
Throttle	0
Datawords	Reason - STRING [200]
Primary Cause	A corruption of the IDX framework for the table has occurred.
Primary Action	Running the **tiat** command indicates whether there is corruption. Fix the corruption.

Monitoring Database Events

This section provides the information you need for monitoring and correcting database events. Table 6-29 lists all of the database events in numerical order and provides cross-references to each subsection.

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

Table 6-29 Cisco BTS 10200 Database Events

Event Type	Event Name	Event Severity
Database (1)	Test Report—Database (1)	Information
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: Back Up 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 Back Up Completed Successfully—Database (19)	Information

Table 6-29 Cisco BTS 10200 Database Events (continued)

Event Type	Event Name	Event Severity
Database (20)	Replication Data Flush Timeout During Switchover—Database (20)	Major
Database (21)	Database Statistics Collection Exception—Database (21)	Minor
Database (22)	Unprovisioned Language—Database (22)	Major
Database (23)	Element Management System Oracle Database—Minor Error—Database (23)	Minor
Database (24)	Element Management System Oracle Database—Major Error—Database (24)	Major
Database (25)	Secure File Transfer Protocol Transfer Failed—Database (25)	Major
Database (26)	File Write Error—Database (26)	Major
Database (27)	Failure Setting the Index Table Soft Limit—Database (27)	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) was not properly completed. 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 6-31.

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 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 6-32.

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 6-32.

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 6-33.

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 6-34.

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 6-34.

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 6-35.

Element Management System Database: Back Up Fails—Database (10)

The Element Management System Database: Back Up Fails alarm (major) indicates that the EMS database back up has failed. To troubleshoot and correct the cause of the Element Management System Database: Back Up Fails alarm, refer to the "Element Management System Database: Back Up Fails—Database (10)" section on page 6-35.

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 6-35.

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 6-35.

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 6-35.

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 6-36.

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 6-36.

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 6-36.

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 6-36.

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.

Daily Database Back Up Completed Successfully—Database (19)

The Daily Database Back Up Completed Successfully event functions as an informational alert that the daily database back up 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 6-36.

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 6-36.

Unprovisioned Language—Database (22)

The Unprovisioned Language alarm (major) indicates that the operator has missed provisioning the language in this alarm in the language table on the EMS. To troubleshoot and correct the cause of the Unprovisioned Language alarm, refer to the "Unprovisioned Language—Database (22)" section on page 6-37.

Element Management System Oracle Database—Minor Error—Database (23)

The Element Management System Oracle Database—Minor Error alarm (minor) indicates that a minor error has occurred in an Oracle background process. To troubleshoot and correct the cause of the Element Management System Oracle Database—Minor Error alarm, refer to the "Element Management System Oracle Database—Minor Error—Database (23)" section on page 6-38.

Element Management System Oracle Database—Major Error—Database (24)

The Element Management System Oracle Database—Major Error alarm (major) indicates that a major error has occurred in an Oracle background process. To troubleshoot and correct the cause of the Element Management System Oracle Database—Major Error alarm, refer to the "Element Management System Oracle Database—Major Error—Database (24)" section on page 6-39.

Secure File Transfer Protocol Transfer Failed—Database (25)

The Secure File Transfer Protocol Transfer Failed alarm (major) indicates that a SFTP file transfer has 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 6-39.

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 6-39.

Failure Setting the Index Table Soft Limit—Database (27)

The Failure Setting the Index Table Soft Limit alarm (major) indicates that a corruption of the IDX framework for the table has occurred. To troubleshoot and correct the cause of the Failure Setting the Index Table Soft Limit alarm, refer to the "Failure Setting the Index Table Soft Limit—Database (27)" section on page 6-39.

Troubleshooting Database Alarms

This section provides the information you need for monitoring and correcting database alarms. Table 6-30 lists all of the database alarms in numerical order and provides cross-references to each subsection.

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

Table 6-30 Cisco BTS 10200 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: Back Up 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 (22)	Unprovisioned Language—Database (22)	Major

Table 6-30 Cisco BTS 10200 Database Alarms (continued)

Alarm Type	Alarm Name	Alarm Severity
Database (23)	Element Management System Oracle Database—Minor Error—Database (23)	Minor
Database (24)	Element Management System Oracle Database—Major Error—Database (24)	Major
Database (25)	Secure File Transfer Protocol Transfer Failed—Database (25)	Major
Database (26)	File Write Error—Database (26)	Major
Database (27)	Failure Setting the Index Table Soft Limit—Database (27)	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 nonexisting data occurred, or a 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.

Prior to contacting Cisco TAC, collect the following information:

On one EMS server:

```
su - oracle
dbadm -C rep
```

On both EMS servers:

```
nodestat
dbadm -r get_deferror
dbadm -r get_deferr
dbadm -r get_deftrandest
dbadm -r get_defcall_order
```

Note Do not perform an EM01 switchover until the deferrors are removed.

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, restart or restore remote database. The secondary cause of the alarm is that a network connection is 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.

For additional troubleshooting information, execute the following:

On one EMS server:

```
su - oracle
dbadm -C rep
```

On both EMS servers:

```
nodestat
dbadm -r get_deferror
dbadm -r get_deferr
dbadm -r get_deftrandest
dbadm -r get_defcall_order
```

Note Do not perform an EM01 switchover until the deferrors are removed.

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.

For additional troubleshooting information, execute the following:

On one EMS server:

```
su - oracle
dbadm -C rep
```

On both EMS servers:

```
nodestat
dbadm -r get_deferror
dbadm -r get_deferr
dbadm -r get_deftrandest
dbadm -r get_defcall_order
```

Note Do not perform an EM01 switchover until the deferrors are removed.

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.

For additional troubleshooting information, execute the following:

On one EMS server:

```
su - oracle
dbadm -C rep
```

On both EMS servers:

```
nodestat
dbadm -r get_deferror
dbadm -r get_deferr
dbadm -r get_deftrandest
dbadm -r get_defcall_order
```

Note Do not perform an EM01 switchover until the deferrors are removed.

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.

For additional troubleshooting information, execute the following:

On one EMS server:

```
su - oracle
dbadm -C rep
```

On both EMS servers:

```
nodestat
dbadm -r get_deferror
dbadm -r get_deferr
dbadm -r get_deftrandest
dbadm -r get_defcall_order
```

Note Do not perform an EM01 switchover until the deferrors are removed.

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.

For additional troubleshooting information, execute the following:

On one EMS server:

```
su - oracle
dbadm -C rep
```

On both EMS servers:

```
nodestat
dbadm -r get_deferror
dbadm -r get_deferr
dbadm -r get_deftrandest
dbadm -r get_defcall_order
```

Note Do not perform an EM01 switchover until the deferrors are removed.

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, back up and clean up the archive log files. Additionally, add more space to archive log directory.

Element Management System Database: Back Up Fails—Database (10)

The Element Management System Database: Back Up Fails alarm (major) indicates that the EMS database back up has failed. The primary cause of the alarm is that the system or hardware is unstable. To correct the primary cause of the alarm, restart the back up 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- errors report in alert.log file is documented in the $ORACLE_HOME/rdbms/mesg/oraus.msg file. Log in to the EMS system as an oracle user (or su - oracle) to view this file. If more information is needed, contact Cisco TAC for database support, or query Oracle metalink library at http://metalink.oracle.com. The corrective action is documented in the $ORACLE_HOME/rdbms/mesg/oraus.msg file. Log in to the EMS system as an oracle user (or su - oracle) to view this file. If more information is needed, contact Cisco TAC for database support, or query the Oracle metalink library at http://metalink.oracle.com. The alert.log file is the global message file for errors issued by all Oracle background processes. The majority of error conditions may require an administrator's investigation and manual correction. Thus the administrator should manually clear this alarm.

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, restart process and contact Cisco TAC.

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.

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 preprovisioned 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.

Prior to contacting Cisco TAC, collect the following information:

```
show db-usage table_name=<string>
```

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.

Unprovisioned Language—Database (22)

The Unprovisioned Language alarm (major) indicates that the operator has missed provisioning the language in this alarm in the language table on the EMS. To correct the cause of the alarm, the operator has to provision the missing language and update the LANGUAGE table.

Use the following procedures to correct the cause of the Unprovisioned Language alarm:

This section describes general troubleshooting procedures.

Ensure the subscriber has MLS using report billing_record:

```
DIALEDDIGITS=*56
CALLTERMINATIONCAUSE=NORMAL_CALL_CLEARING
```

*56 is the VSC entered by the subscriber to start MLS. NORMAL_CALL_CLEARING shows the IVR successfully completed its service.

If NORMAL_CALL_CLEARING does not return, check both the service and subscriber_service_profile tables:

```
btsadmin> show service id=mlstest
ID=mlstest
FNAME1=MLS

btsadmin> show subscriber_service_profile sub-id=2212437211
SUB_ID=2212437211
SERVICE_ID=mlstest
```

If you hear a reorder-tone from a SIP phone, ensure the status of the Cisco BTS 10200 announcement table is all of the following:

```
btsadmin> status tt tgn-id=889; cic=all
889 1   ADMIN_INS     TERM_ACTIVE_IDLE      ACTV   IDLE   NON_FAULTY
```

If you hear a click from an MGCP phone, ensure the status of the Cisco BTS 10200 announcement table is all of the following:

```
btsadmin> status tt tgn-id=889;cic=all
889 1   ADMIN_INS     TERM_ACTIVE_IDLE      ACTV   IDLE   NON_FAULTY
```

If you hear a reorder tone instead of audio, ensure the release_cause table routes to correct MS:

```
btsadmin> show release_cause
ID=1
ANNC_ID=18
btsadmin> show announcement
...
ANNOUNCEMENT_FILE=ann_id_18.au
ROUTE_GUIDE_ID=10013
```

Ensure the IVR script points to the correct MS and that the MLS has an FNAME:

```
btsadmin> show ivr_script_profile
FNAME=MLS
IVR_ACCESS_MODE=IVR
IVR_ROUTE_GUIDE_ID=10013
IVR_SCRIPT_PKG_TYPE=BAU
```

Ensure the annc-tg-profile table is correct:

```
ANNC_LANG_FORMAT_SUPPORTED=N for IPUnity
ANNC_LANG_FORMAT_SUPPORTED=Y for Cognitronics
```

Turn on trace in the Cisco BTS 10200 Call Agent (CA) for MLS, set MGCP on the CA to info5 level, and examine the BAU code from the MS:

```
TC_11.3.1_CA.log:..           MGA    00-00.           |<<<< RECV FROM: 10.1.31.2
FROM-PORT=2427 TO-PORT=2727 <<<<|

TC_11.3.1_CA.log-..           MGA    00-00.           |ntfy 717
annc/1@sj-ms1-s4.sjc-devtest.com MGCP 1.0 NCS 1.0^M|

TC_11.3.1_CA.log-..           MGA    00-00.           |X: 2B00000007^M|

TC_11.3.1_CA.log-..           MGA    00-00.           |O: A/of(rc=601)^M|
TC_11.3.1_CA.log-..           MGA    00-00.           ||snd_rcv.c:260

Error:    NEED
```

Explanation:

The mls-annc-mult-factor token value is lower than the number of announcements existing on the MS.

Recommended Action:

Provision the mls-annc-mult-factor token value greater than the number of announcements on the MS.

```
Error: Return Code 601: File not found
```

Explanation:

MSs are limited to 40 character filenames. These 40 characters include the extension (typically a wav) and the announcement-file-prefix: for example fra_, eng_ and spa_.

Recommended Action:

Change the filename length to less than 40 characters.

Element Management System Oracle Database—Minor Error—Database (23)

The Element Management System Oracle Database—Minor Error alarm (minor) indicates that a minor error has occurred in an Oracle background process. The probable cause of the ORA- errors report in alert.log file is documented in the $ORACLE_HOME/rdbms/mesg/oraus.msg file. Log in to the EMS system as an oracle user (or su - oracle) to view this file. If more information is needed, contact Cisco TAC for database support, or query the Oracle metalink library at http://metalink.oracle.com. The corrective action is documented in the $ORACLE_HOME/rdbms/mesg/oraus.msg file. Log in to the EMS system as an oracle user (or su - oracle) to view this file. If more information is needed, contact Cisco TAC for database support, or query the Oracle metalink library at http://metalink.oracle.com. The alert.log file is the global message file for errors issued by all Oracle background processes. The majority of error conditions may require an administrator's investigation and manual correction. Thus the administrator should manually clear this alarm.

Element Management System Oracle Database—Major Error—Database (24)

The Element Management System Oracle Database—Major Error alarm (major) indicates that a major error has occurred in an Oracle background process. The probable cause of the ORA- errors report in alert.log file is documented in the $ORACLE_HOME/rdbms/mesg/oraus.msg file. Log in to the EMS system as an oracle user (or su - oracle) to view this file. If more information is needed, contact Cisco TAC for database support, or query the Oracle metalink library at http://metalink.oracle.com. The corrective action is documented in the $ORACLE_HOME/rdbms/mesg/oraus.msg file. Log in to the EMS system as an oracle user (or su - oracle) to view this file. If more information is needed, contact Cisco TAC for database support, or query the Oracle metalink library at http://metalink.oracle.com. The alert.log file is the global message file for errors issued by all Oracle background processes. The majority of error conditions may require an administrator's investigation and manual correction. Thus the administrator should manually clear this alarm.

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 establish a communication channel between the active and the standby call agent. To troubleshoot and correct the primary cause of the alarm, check the communication channel between the primary and the secondary call agent (CA). On each CA, ping the other node. The secondary cause of the alarm is that the system was unable to log in to the remote host. To troubleshoot and correct the secondary cause of the alarm, verify that the SSH keys have been preconfigured 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.

Failure Setting the Index Table Soft Limit—Database (27)

The Failure Setting the Index Table Soft Limit alarm (major) indicates that a corruption of the IDX framework for the table has occurred. To troubleshoot and correct the primary cause of the alarm, run the **tiat** command to verify that a corruption has occurred. Once the corruption is verified, fix the corruption.

CHAPTER 7

Maintenance Troubleshooting

Revised: August 10, 2011, OL-25016-01

Introduction

This chapter provides the information needed for monitoring and troubleshooting 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 for monitoring and correcting the maintenance events
- Troubleshooting Maintenance Alarms—Provides the information needed for troubleshooting and correcting the maintenance alarms

Maintenance Events and Alarms

This section provides a brief overview of the maintenance events and alarms for the Cisco BTS 10200 Softswitch; the event and alarms are arranged in numerical order. Table 7-1 lists all of the maintenance events and alarms by severity.

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

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	Information	Not Used
Maintenance (40)	Maintenance (3)	Maintenance (18)	Maintenance (29)	Maintenance (1)	Maintenance (31)
Maintenance (43)	Maintenance (4)	Maintenance (24)	Maintenance (41)	Maintenance (2)	Maintenance (59)
Maintenance (44)	Maintenance (5)	Maintenance (48)	Maintenance (75)	Maintenance (11)	Maintenance (60)
Maintenance (47)	Maintenance (6)	Maintenance (67)	Maintenance (108)	Maintenance (12)	Maintenance (76)
Maintenance (50)	Maintenance (7)	Maintenance (83)	Maintenance (123)	Maintenance (13)	Maintenance (105)
Maintenance (53)	Maintenance (8)	Maintenance (86)		Maintenance (14)	Maintenance (106)
Maintenance (57)	Maintenance (9)	Maintenance (90)		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 (117)	Maintenance (71)			Maintenance (52)	
Maintenance (118)	Maintenance (72)			Maintenance (54)	

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

Critical	Major	Minor	Warning	Information	Not Used
Maintenance (119)	Maintenance (77)			Maintenance (56)	
Maintenance (126)	Maintenance (84)			Maintenance (58)	
Maintenance (127)	Maintenance (87)			Maintenance (78)	
	Maintenance (88)			Maintenance (79)	
	Maintenance (89)			Maintenance (80)	
	Maintenance (92)			Maintenance (81)	
	Maintenance (93)			Maintenance (94)	
	Maintenance (99)			Maintenance (95)	
	Maintenance (109)			Maintenance (96)	
	Maintenance (110)			Maintenance (104)	
	Maintenance (112)			Maintenance (113)	
				Maintenance (114)	
				Maintenance (115)	
				Maintenance (116)	
				Maintenance (120)	
				Maintenance (121)	
				Maintenance (122)	

Maintenance (1)

Table 7-2 lists the details of the Maintenance (1) informational event. For additional information, refer to the "Test Report—Maintenance (1)" section on page 7-75.

Table 7-2 Maintenance (1) Details

Description	Test Report
Severity	Information
Threshold	10000
Throttle	0

Maintenance (2)

Table 7-3 lists the details of the Maintenance (2) informational event. For additional information, refer to the "Report Threshold Exceeded—Maintenance (2)" section on page 7-75.

Table 7-3 Maintenance (2) Details

Description	Report Threshold Exceeded
Severity	Information
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 and the threshold setting should be investigated to determine if there is a service-affecting situation.

Maintenance (3)

Table 7-4 lists the details of the Maintenance (3) major alarm. To troubleshoot and correct the cause of the alarm, refer to the "Local Side Has Become Faulty—Maintenance (3)" section on page 7-99.

Table 7-4 Maintenance (3) Details

Description	Keep Alive Module: Local Side Has Become Faulty (KAM: Local Side Has Become Faulty)
Severity	Major
Threshold	100
Throttle	0
Datawords	Local State—STRING [30] Mate State—STRING [30] Reason—STRING [80] Probable Cause—STRING [80]
Primary Cause	Can result from maintenance report 5, 6, 9, 10, 19, or 20.
Primary Action	Review the information from the command line interface (CLI) log report. Usually a software problem; restart the software using the installation and startup procedure.
Secondary Cause	Manually shutting down the system using **platform stop** command.
Secondary Action	Reboot the host machine, reinstall all applications and restart all applications. If the fault state is a commonly occurring problem, then the operating system (OS) or a hardware failure may be the problem.

Maintenance (4)

Table 7-5 lists the details of the Maintenance (4) major alarm. To troubleshoot and correct the cause of the alarm, refer to the "Mate Side Has Become Faulty—Maintenance (4)" section on page 7-99.

Table 7-5 Maintenance (4) Details

Description	Keep Alive Module: Mate Side Has Become Faulty (KAM: Mate Side Has Become Faulty)
Severity	Major
Threshold	100
Throttle	0
Datawords	Local State—STRING [30] Mate State—STRING [30] Reason—STRING [80] Probable Cause—STRING [80] Mate Ping—STRING [50]
Primary Cause	The local side has detected the mate side going to the faulty state.
Primary Action	Display the event summary on the faulty mate side, using the **report event-summary** command (see the Cisco BTS 10200 Softswitch CLI Database for command details).
Secondary Action	Review the 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 the **platform stop** command and then the **platform start** command.
Subsequent Action	If software restart does not resolve the problem or 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 the OS or a hardware failure may be the problem. Reboot the host machine, then reinstall and restart all applications. Rebooting brings down other applications running on this machine. Contact Cisco TAC for assistance.

Maintenance (5)

Table 7-6 lists the details of the Maintenance (5) major alarm. To troubleshoot and correct the cause of the alarm, refer to the "Changeover Failure—Maintenance (5)" section on page 7-99.

Table 7-6 Maintenance (5) Details

Description	Keep Alive Module: Changeover Failure (KAM: 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	Restart the platform identified in the alarm report.
Ternary Action	If platform restart is not successful, reinstall the application for this platform, and then restart platform again.
Subsequent Action	If necessary, reboot host machine this platform is located on. Then reinstall and restart all applications on this machine. If faulty state is a commonly occurring event, then the OS or a hardware failure may be the problem. Contact Cisco TAC for assistance. It may also be helpful to gather information from event and alarm reports that were issued before and after this alarm report.

Maintenance (6)

Table 7-7 lists the details of the Maintenance (6) major alarm. To troubleshoot and correct the cause of the alarm, refer to the "Changeover Timeout—Maintenance (6)" section on page 7-100.

Table 7-7 Maintenance (6) Details

Description	Keep Alive Module: Changeover Timeout (KAM: Changeover Timeout)
Severity	Major
Threshold	100
Throttle	0
Datawords	Local State—STRING [30] Mate State—STRING [30]
Primary Cause	The system failed to changeover within the required time period. Soon after this event is issued, one platform will go to the faulty state.
Primary Action	Review the 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	Restart the platform identified in the alarm report.
Ternary Action	If platform restart is not successful, reinstall the application for this platform, and then restart the platform again.
Subsequent Action	If necessary, reboot the host machine this platform is located on. Then reinstall and restart all applications on this machine. If faulty state is a commonly occurring event, then the operating system (OS) or a hardware failure may be the problem. Contact Cisco TAC for assistance. It may also be helpful to gather information from event and alarm reports that were issued before and after this alarm report.

Maintenance (7)

Table 7-8 lists the details of the Maintenance (7) major alarm. To troubleshoot and correct the cause of the alarm, refer to the "Mate Rejected Changeover—Maintenance (7)" section on page 7-100.

Table 7-8 Maintenance (7) Details

Description	Keep Alive Module: Mate Rejected Changeover (KAM: 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	The 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 while the primary instance is being brought up.
Secondary Action	If the 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, determine whether both instances are operating in a 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 the 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.

Maintenance (8)

Table 7-9 lists the details of the Maintenance (8) major alarm. To troubleshoot and correct the cause of the alarm, refer to the "Mate Changeover Timeout—Maintenance (8)" section on page 7-103.

Table 7-9 Maintenance (8) Details

Description	Keep Alive Module: Mate Changeover Timeout (KAM: Mate Changeover Timeout)
Severity	Major
Threshold	100
Throttle	0
Datawords	Local State—STRING [30] Mate State—STRING [30]
Primary Cause	The mate is faulty.
Primary Action	Review the information from CLI log report concerning the 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	Restart the mate platform identified in the alarm report.
Subsequent Action	If mate platform restart is not successful, reinstall the application for this mate platform, and then restart the mate platform again. If necessary, reboot the host machine this mate platform is located on. Then reinstall and restart all applications on that machine.

Maintenance (9)

Table 7-10 lists the details of the Maintenance (9) major alarm. To troubleshoot and correct the cause of the alarm, refer to the "Local Initialization Failure—Maintenance (9)" section on page 7-103.

Table 7-10 Maintenance (9) Details

Description	Keep Alive Module: Local Initialization Failure (KAM: Local Initialization Failure)
Severity	Major
Threshold	100
Throttle	0
Datawords	Local State—STRING [30] Mate State—STRING [30]
Primary Cause	The local initialization has failed.
Primary Action	When this event report is issued, the system has failed and the reinitialization 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 reinstall the files from the initial or back up media. Then restart the failed device.

Maintenance (10)

Table 7-11 lists the details of the Maintenance (10) major alarm. To troubleshoot and correct the cause of the alarm, refer to the "Local Initialization Timeout—Maintenance (10)" section on page 7-103.

Table 7-11 Maintenance (10) Details

Description	Keep Alive Module: Local Initialization Timeout (KAM: Local Initialization Timeout)
Severity	Major
Threshold	100
Throttle	0
Datawords	Local State—STRING [30] Mate State—STRING [30]
Primary Cause	The 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 reinitialization process has failed.
Secondary Action	If the files are not present, then reinstall the files from the initial or back up media. Then restart the failed device.

Maintenance (11)

Table 7-12 lists the details of the Maintenance (11) informational event. For additional information, refer to the "Switchover Complete—Maintenance (11)" section on page 7-76.

Table 7-12 Maintenance (11) Details

Description	Switchover Complete
Severity	Information
Threshold	100
Throttle	0
Datawords	Local State—STRING [30] Mate State—STRING [30]
Primary Cause	Acknowledges that the changeover has successfully completed.
Primary Action	This is an informational event report and no further action is required.

Maintenance (12)

Table 7-13 lists the details of the Maintenance (12) informational event. For additional information, refer to the "Initialization Successful—Maintenance (12)" section on page 7-76.

Table 7-13 Maintenance (12) Details

Description	Keep Alive Module: Initialization Successful (KAM: Initialization Successful)
Severity	Information
Threshold	100
Throttle	0
Datawords	Local State—STRING [30] Mate State—STRING [30]
Primary Cause	The local initialization has been successfully completed.
Primary Action	This an informational event report and no further action is required.

Maintenance (13)

Table 7-14 lists the details of the Maintenance (13) informational event. For additional information, refer to the "Administrative State Change—Maintenance (13)" section on page 7-76.

Table 7-14 Maintenance (13) Details

Description	Administrative State Change (Admin State Change)
Severity	Information
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, because this informational event report is given after a user has manually changed the administrative state of a managed resource.

Maintenance (14)

Table 7-15 lists the details of the Maintenance (14) informational event. For additional information, refer to the "Call Agent Administrative State Change—Maintenance (14)" section on page 7-77.

Table 7-15 Maintenance (14) Details

Description	Call Agent Administrative State Change
Severity	Information
Threshold	100
Throttle	0
Datawords	Call Agent ID—STRING [40] Current Local State—STRING [40] Current Mate State—STRING [20]
Primary Cause	Indicates that the 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)

Table 7-16 lists the details of the Maintenance (15) informational event. For additional information, refer to the "Feature Server Administrative State Change—Maintenance (15)" section on page 7-77.

Table 7-16 Maintenance (15) Details

Description	Feature Server Administrative State Change
Severity	Information
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 the 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)

Table 7-17 lists the details of the Maintenance (16) informational event. For additional information, refer to the "Process Manager: Process Has Died: Starting Process—Maintenance (16)" section on page 7-77.

Table 7-17 Maintenance (16) Details

Description	Process Manager: Starting Process (PMG: Starting Process)
Severity	Information
Threshold	100
Throttle	0
Datawords	Process Name—STRING [40] Restart Type—STRING [40] Restart Mode—STRING [32] Process Group—ONE_BYTE
Primary Cause	A process is being started as the system is being brought up.
Primary Action	No action is required.

Maintenance (17)

Table 7-18 lists the details of the Maintenance (17) informational event. For additional information, refer to the "Invalid Event Report Received—Maintenance (17)" section on page 7-77.

Table 7-18 Maintenance (17) Details

Description	Invalid Event Report Received
Severity	Information
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 is 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.

Maintenance (18)

Table 7-19 lists the details of the Maintenance (18) minor alarm. To troubleshoot and correct the cause of the alarm, refer to the "Process Manager: Process Has Died—Maintenance (18)" section on page 7-103.

Table 7-19 Maintenance (18) Details

Description	Process Manager: Process Has Died (PMG: Process has Died)
Severity	Minor
Threshold	100
Throttle	0
Datawords	Process Name—STRING [40] Process Group—FOUR_BYTES
Primary Cause	This alarm is caused by a software problem.
Primary Action	If problem persists, contact Cisco TAC technical support.

Maintenance (19)

Table 7-20 lists the details of the Maintenance (19) major alarm. To troubleshoot and correct the cause of the alarm, refer to the "Process Manager: Process Exceeded Restart Rate—Maintenance (19)" section on page 7-103.

Table 7-20 Maintenance (19) Details

Description	Process Manager: Process Exceeded Restart Rate (PMG: 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 the faulty state.
Primary Action	Review the information from CLI log report.
Secondary Action	Restart the platform identified in the alarm report.
Ternary Action	If platform restart is not successful, reinstall the application for this platform, and then restart platform again.
Subsequent Action	If necessary, reboot the host machine this platform is located on. Then reinstall and restart all applications on this machine.

Maintenance (20)

Table 7-21 lists the details of the Maintenance (20) major alarm. To troubleshoot and correct the cause of the alarm, refer to the "Lost Connection to Mate—Maintenance (20)" section on page 7-104.

Table 7-21 Maintenance (20) Details

Description	Keep Alive Module: Lost Connection to Mate (KAM: Lost KAM Connection to Mate)
Severity	Major
Threshold	100
Throttle	0
Datawords	Mate Ping—STRING [50]
Primary Cause	Network interface hardware problem.
Primary Action	Check whether or not the network interface is down. If it is down, restore network interface and restart the software.
Secondary Cause	The alarm can be caused by a router problem.
Secondary Action	If the alarm is caused by a router problem, repair the router and reinstall.
Ternary Cause	Soon after this event is issued, one platform may go to the faulty state.

Maintenance (21)

Table 7-22 lists the details of the Maintenance (21) major alarm. To troubleshoot and correct the cause of the alarm, refer to the "Network Interface Down—Maintenance (21)" section on page 7-104.

Table 7-22 Maintenance (21) Details

Description	Keep Alive Module: Network Interface Down (KAM: Network Interface Down)
Severity	Major
Threshold	100
Throttle	0
Datawords	IP Address—STRING [50]
Primary Cause	The alarm is caused by a network interface hardware problem.
Primary Action	Check and correct for problems with the network interfaces.
Secondary Cause	Soon after this event is issued, one platform may go to the faulty state.
Secondary Action	Check whether or not the network interface is down. If the interface is down, restore network interface and restart the software.

Maintenance (22)

Table 7-23 lists the details of the Maintenance (22) informational event. For additional information, refer to the "Mate Is Alive—Maintenance (22)" section on page 7-78.

Table 7-23 Maintenance (22) Details

Description	Keep Alive Module: Mate Is Alive (KAM: Mate is Alive)
Severity	Information
Threshold	100
Throttle	0
Datawords	Local State—STRING [30] Mate State—STRING [30]

Maintenance (23)

Table 7-24 lists the details of the Maintenance (23) major alarm. To troubleshoot and correct the cause of the alarm, refer to the "Process Manager: Process Failed to Complete Initialization—Maintenance (23)" section on page 7-104.

Table 7-24 Maintenance (23) Details

Description	Process Manager: Process Failed to Complete Initialization (PMG: Process Failed to Complete Initialization)
Severity	Major
Threshold	100
Throttle	0
Datawords	Process Name—STRING [40] Process Group—ONE_BYTE
Primary Cause	The specified process failed to complete the initialization during the restoration process.
Primary Action	Verify that the specified process's binary image is installed. If not, install it and restart the platform.

Maintenance (24)

Table 7-25 lists the details of the Maintenance (24) minor alarm. To troubleshoot and correct the cause of the alarm, refer to the "Process Manager: Restarting Process—Maintenance (24)" section on page 7-104.

Table 7-25 Maintenance (24) Details

Description	Process Manager: Restarting Process (PMG: 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	The software process has exited abnormally and had to be restarted.
Primary Action	If the problem persists, contact Cisco TAC.

Maintenance (25)

Table 7-26 lists the details of the Maintenance (25) informational event. For additional information, refer to the "Process Manager: Changing State—Maintenance (25)" section on page 7-78.

Table 7-26 Maintenance (25) Details

Description	Process Manager: Changing State (PMG: Changing State)
Severity	Information
Threshold	100
Throttle	0
Datawords	Platform State—STRING [40]

Maintenance (26)

Table 7-27 lists the details of the Maintenance (26) major alarm. To troubleshoot and correct the cause of the alarm, refer to the "Process Manager: Going Faulty—Maintenance (26)" section on page 7-104.

Table 7-27 Maintenance (26) Details

Description	Process Manager: Going Faulty (PMG: Going Faulty)
Severity	Major
Threshold	100
Throttle	0
Datawords	Reason—STRING [40]
Primary Cause	The system has been brought down because the system has detected a fault.
Primary Action	If it is not due to the operator intentionally bringing down the system, then the platform has detected a fault and has shut down. This is typically followed by a Maintenance (3) alarm event. Use corrective action procedures provided for the Maintenance (3) alarm event.

Maintenance (27)

Table 7-28 lists the details of the Maintenance (27) informational event. For additional information, refer to the "Process Manager: Changing Over to Active—Maintenance (27)" section on page 7-79.

Table 7-28 Maintenance (27) Details

Description	Process Manager: Changing Over to Active (PMG: Changing Over to Active)
Severity	Information
Threshold	100
Throttle	0

Maintenance (28)

Table 7-29 lists the details of the Maintenance (28) informational event. For additional information, refer to the "Process Manager: Changing Over to Standby—Maintenance (28)" section on page 7-79.

Table 7-29 Maintenance (28) Details

Description	Process Manager: Changing Over to Standby (PMG: Changing Over to Standby)
Severity	Information
Threshold	100
Throttle	0

Maintenance (29)

Table 7-30 lists the details of the Maintenance (29) warning event. To monitor and correct the cause of the event, refer to the "Administrative State Change Failure—Maintenance (29)" section on page 7-79.

Table 7-30 Maintenance (29) Details

Description	Administrative State Change Failure (Admin 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	Analyze the cause of the failure if a cause is found. Verify that the controlling element of the targeted device was in the active state in order to service the request to change the adminstrator state of the device.
Ternary Action	If the controlling platform instance is not active, restore it to service.

Maintenance (30)

Table 7-31 lists the details of the Maintenance (30) informational event. For additional information, refer to the "Element Manager State Change—Maintenance (30)" section on page 7-79.

Table 7-31 Maintenance (30) Details

Description	Element Manager State Change
Severity	Information
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 been changed to the indicated state either naturally or through a 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.

Maintenance (31)

Maintenance (31) is not used.

Maintenance (32)

Table 7-32 lists the details of the Maintenance (32) informational event. For additional information, refer to the "Process Manager: Sending Go Active to Process—Maintenance (32)" section on page 7-79.

Table 7-32 Maintenance (32) Details

Description	Process Manager: Sending Go Active to Process (PMG: Sending Go Active to Process)
Severity	Information
Threshold	100
Throttle	0
Datawords	Process Name—STRING [40] Process Group—ONE_BYTE
Primary Cause	Process is being notified to switch to the active state because the system is switching over from the standby state to the active state.
Primary Action	No action is necessary.

Maintenance (33)

Table 7-33 lists the details of the Maintenance (33) informational event. For additional information, refer to the "Process Manager: Sending Go Standby to Process—Maintenance (33)" section on page 7-79.

Table 7-33 Maintenance (33) Details

Description	Process Manager: Sending Go Standby to Process (PMG: Sending Go Standby to Process)
Severity	Information
Threshold	100
Throttle	0
Datawords	Process Name—STRING [40] Process Group—ONE_BYTE
Primary Cause	The process is being notified to exit gracefully because the system is switching over to the standby state, or it is shutting down. The switchover or shutdown could be due to either of the following: (1) The 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)

Table 7-34 lists the details of the Maintenance (34) informational event. For additional information, refer to the "Process Manager: Sending End Process to Process—Maintenance (34)" section on page 7-80.

Table 7-34 Maintenance (34) Details

Description	Process Manager: Sending End Process to Process (PMG: Sending End Process to Process)
Severity	Information
Threshold	100
Throttle	0
Datawords	Process Name—STRING [40] Process Group—ONE_BYTE
Primary Cause	The process is being notified to exit gracefully because the system is switching over to the standby state, or it is shutting down. The switchover or shutdown could be due to either of the following: (1) The 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)

Table 7-35 lists the details of the Maintenance (35) informational event. For additional information, refer to the "Process Manager: All Processes Completed Initialization—Maintenance (35)" section on page 7-80.

Table 7-35 Maintenance (35) Details

Description	Process Manager: All Processes Completed Initialization (PMG: All Processes Completed Initialization)
Severity	Information
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)

Table 7-36 lists the details of the Maintenance (36) informational event. For additional information, refer to the "Process Manager: Sending All Processes Initialization Complete to Process—Maintenance (36)" section on page 7-80.

Table 7-36 Maintenance (36) Details

Description	Process Manager: Sending All Processes Initialization Complete to Process (PMG: Sending All Processes Init Complete to Process)
Severity	Information
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)

Table 7-37 lists the details of the Maintenance (37) informational event. For additional information, refer to the "Process Manager: Killing Process—Maintenance (37)" section on page 7-80.

Table 7-37 Maintenance (37) Details

Description	Process Manager: Killing Process (PMG: Killing Process)
Severity	Information
Threshold	100
Throttle	0
Datawords	Process Name—STRING [40] Process Group—ONE_BYTE
Primary Cause	A software problem 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)

Table 7-38 lists the details of the Maintenance (38) informational event. For additional information, refer to the "Process Manager: Clearing the Database—Maintenance (38)" section on page 7-80.

Table 7-38 Maintenance (38) Details

Description	Process Manager: Clearing the Database (PMG: Clearing the Database)
Severity	Information
Threshold	100
Throttle	0
Primary Cause	The system is preparing to copy data from the mate. (The system has been brought up and the mate side is running.)
Primary Action	No action is necessary.

Maintenance (39)

Table 7-39 lists the details of the Maintenance (39) informational event. For additional information, refer to the "Process Manager: Cleared the Database—Maintenance (39)" section on page 7-80.

Table 7-39 Maintenance (39) Details

Description	Process Manager: Cleared the Database (PMG: Cleared the Database)
Severity	Information
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)

Table 7-40 lists the details of the Maintenance (40) critical alarm. 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 7-105.

Table 7-40 Maintenance (40) Details

Description	Process Manager: Binary Does not Exist for Process (PMG: Binary Does not Exist for Process)
Severity	Critical
Threshold	100
Throttle	0
Datawords	Program Name—STRING [30] Executable Name—STRING [100]
Primary Cause	The platform is not installed correctly.
Primary Action	Reinstall the platform.

Maintenance (41)

Table 7-41 lists the details of the Maintenance (41) warning event. To monitor and correct the cause of the event, refer to the "Administrative State Change Successful With Warning—Maintenance (41)" section on page 7-81.

Table 7-41 Maintenance (41) Details

Description	Administrative State Change Successful With Warning (Admin 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	The device was in a flux state.
Primary Action	Retry the administrative state change.

Maintenance (42)

Table 7-42 lists the details of the Maintenance (42) major alarm. 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 7-105.

Table 7-42 Maintenance (42) Details

Description	Keep Alive Module: Number of Heartbeat Messages Received is Less Than 50% of Expected (KAM: # of HB Messages Received is Less Than 50% of Expected)
Severity	Major
Threshold	100
Throttle	0
Datawords	Interface Name—STRING [50] IP Address—STRING [50] Expected HB Messages—ONE_BYTE HB Messages Received—ONE_BYTE
Primary Cause	The alarm is caused by a network problem.
Primary Action	Fix the network problem.

Maintenance (43)

Table 7-43 lists the details of the Maintenance (43) critical alarm. 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 7-105.

Table 7-43 Maintenance (43) Details

Description	Process Manager: Process Failed to Come Up in Active Mode (PMG: Process Failed to Come Up in Active Mode)
Severity	Critical
Threshold	100
Throttle	0
Datawords	Process Name—STRING [40] Process Group—ONE_BYTE
Primary Cause	The alarm is caused by a software or a configuration problem.
Primary Action	Restart the platform. If the problem persists contact Cisco TAC.

Maintenance (44)

Table 7-44 lists the details of the Maintenance (44) critical alarm. 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 7-105.

Table 7-44 Maintenance (44) Details

Description	Process Manager: Process Failed to Come Up in Standby Mode (PMG: Process Failed to Come Up in Standby Mode)
Severity	Critical
Threshold	100
Throttle	0
Datawords	Process Name—STRING [40] Process Group—ONE_BYTE
Primary Cause	The alarm is caused by a software or a configuration problem.
Primary Action	Restart the platform. If the problem persists contact Cisco TAC.

Maintenance (45)

Table 7-45 lists the details of the Maintenance (45) major alarm. To troubleshoot and correct the cause of the alarm, refer to the "Application Instance State Change Failure—Maintenance (45)" section on page 7-105.

Table 7-45 Maintenance (45) Details

Description	Application Instance State Change Failure
Severity	Major
Threshold	100
Throttle	0
Datawords	Application Instance—STRING [20] Failure Reason—STRING [80]
Primary Cause	The switchover of an application instance failed because of a platform fault.
Primary Action	Retry the switchover and if the condition continues contact Cisco TAC.

Maintenance (46)

Table 7-46 lists the details of the Maintenance (46) informational event. For additional information, refer to the "Network Interface Restored—Maintenance (46)" section on page 7-82.

Table 7-46 Maintenance (46) Details

Description	Network Interface Restored
Severity	Information
Threshold	100
Throttle	0
Datawords	Interface Name—STRING [80] Interface IP Address—STRING [80]
Primary Cause	The interface cable is reconnected and interface is restored using the **ifconfig up** command.
Primary Action	No action is required.

Maintenance (47)

Table 7-47 lists the details of the Maintenance (47) critical alarm. To troubleshoot and correct the cause of the alarm, refer to the "Thread Watchdog Counter Expired for a Thread—Maintenance (47)" section on page 7-105.

Table 7-47 Maintenance (47) Details

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	The alarm is caused by a software error.
Primary Action	No action is required. (The system will automatically recover or shut down.)

Maintenance (48)

Table 7-48 lists the details of the Maintenance (48) minor alarm. 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 7-106.

Table 7-48 Maintenance (48) Details

Description	Index Table Usage Exceeded Minor Usage Threshold Level (IDX Table Usage Exceeded Minor Usage Threshold Level)
Severity	Minor
Threshold	100
Throttle	0
Datawords	Table Name—STRING [80] Size—FOUR_BYTES Used—FOUR_BYTES
Primary Cause	Call traffic volume is above the design limits.
Primary Action	Verify that the traffic is within the rated capacity.
Secondary Cause	A software problem requiring manufacture analysis has occurred.
Secondary Action	Contact Cisco TAC.

Maintenance (49)

Table 7-49 lists the details of the Maintenance (49) major alarm. 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 7-106.

Table 7-49 Maintenance (49) Details

Description	Index Table Usage Exceeded Major Usage Threshold Level (IDX Table Usage Exceeded Major Usage Threshold Level)
Severity	Major
Threshold	100
Throttle	0
Datawords	Table Name—STRING [80] Table Size—FOUR_BYTES Used—FOUR_BYTES
Primary Cause	Call traffic volume is above the design limits.
Primary Action	Verify that the traffic is within rated capacity.
Secondary Cause	A software problem requiring manufacture analysis has occurred.
Secondary Action	Contact Cisco TAC.

Maintenance (50)

Table 7-50 lists the details of the Maintenance (50) critical alarm. 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 7-106.

Table 7-50 Maintenance (50) Details

Description	Index Table Usage Exceeded Critical Usage Threshold Level (IDX Table Usage Exceeded Critical Usage Threshold Level)
Severity	Critical
Threshold	100
Throttle	0
Datawords	Table Name—STRING [80] Table Size—FOUR_BYTES Used—FOUR_BYTES
Primary Cause	Call traffic volume is above the design limits.
Primary Action	Verify that the traffic is within rated capacity.
Secondary Cause	A software problem requiring manufacture analysis has occurred.
Secondary Action	Contact Cisco TAC.

Maintenance (51)

Table 7-51 lists the details of the Maintenance (51) major alarm. 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 7-106.

Table 7-51 Maintenance (51) Details

Description	A Process Exceeds 70% of Central Processing Unit Usage (A Process Exceeds 70% of CPU Usage)
Severity	Major
Threshold	100
Throttle	0
Datawords	Host Name—STRING [40] 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)

Table 7-52 lists the details of the Maintenance (52) informational event. For additional information, refer to the "Central Processing Unit Usage Is Now Below the 50% Level—Maintenance (52)" section on page 7-83.

Table 7-52 Maintenance (52) Details

Description	Central Processing Unit Usage Is Now Below the 50% Level (CPU Usage Is Now Below the 50% Level)
Severity	Information
Threshold	100
Throttle	0
Datawords	Host Name—STRING [40] PID—STRING [40] Process Name—STRING [40] CPU Usage—STRING [40]
Primary Cause	This is an informational event and no troubleshooting is necessary.
Primary Action	No corrective action is necessary.

Maintenance (53)

Table 7-53 lists the details of the Maintenance (53) critical alarm. 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 7-106.

Table 7-53 Maintenance (53) Details

Description	The Central Processing Unit Usage Is Over 90% Busy (The CPU Usage Is Over 90% Busy)
Severity	Critical
Threshold	100
Throttle	0
Datawords	Host Name—STRING [40] CPU Usage—STRING [40]
Primary Cause	Too numerous to determine.
Primary Action	Try to isolate the problem. Contact Cisco TAC for assistance.

Maintenance (54)

Table 7-54 lists the details of the Maintenance (54) informational event. For additional information, refer to the "The Central Processing Unit Has Returned to Normal Levels of Operation—Maintenance (54)" section on page 7-83.

Table 7-54 Maintenance (54) Details

Description	The Central Processing Unit Has Returned to Normal Levels of Operation (The CPU Has Returned to Normal Levels of Operation)
Severity	Information
Threshold	100
Throttle	0
Datawords	Host Name—STRING [40] CPU Usage—STRING [40]
Primary Cause	Not applicable.
Primary Action	Not applicable.

Maintenance (55)

Table 7-55 lists the details of the Maintenance (55) major alarm. 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 7-107.

Table 7-55 Maintenance (55) Details

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 that all subsystems are performing normally. If they are, only lightening the effective load on the system will clear the situation. If they are not, verify which process(es) are running at abnormally high rates and provide the information to Cisco TAC.

Maintenance (56)

Table 7-56 lists the details of the Maintenance (56) informational event. For additional information, refer to the "The Load Average Has Returned to Normal Levels—Maintenance (56)" section on page 7-83.

Table 7-56 Maintenance (56) Details

Description	The Load Average Has Returned to Normal Levels
Severity	Information
Threshold	100
Throttle	0
Datawords	Host Name—STRING [40] Load Average—STRING [40]
Primary Cause	Not applicable.
Primary Action	Not applicable.

Maintenance (57)

Table 7-57 lists the details of the Maintenance (57) critical alarm. 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 7-107.

Note Maintenance (57) is issued by the Cisco BTS 10200 system when memory consumption is greater than 95 percent (>95%) and swap space consumption is greater than 50 percent (>50%).

Table 7-57 Maintenance (57) Details

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 that all subsystems are performing normally. If they are, only lightening the effective load on the system will clear the situation. If they are not, verify which process(es) are running at abnormally high rates and provide the information to Cisco TAC.

Maintenance (58)

Table 7-58 lists the details of the Maintenance (58) informational event. For additional information, refer to the "Memory and Swap Are Consumed at Abnormal Levels—Maintenance (58)" section on page 7-84.

Note Maintenance (58) is issued by the Cisco BTS 10200 system when memory consumption is greater than 80 percent (>80%) and swap space consumption is greater than 30 percent (>30%).

Table 7-58 Maintenance (58) Details

Description	Memory and Swap Are Consumed at Abnormal Levels
Severity	Information
Threshold	100
Throttle	0
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 they are, only lightening the effective load on the system will clear the situation. If they are not, verify which process(es) are running at abnormally high rates and provide the information to Cisco TAC.

Maintenance (59)

Maintenance (59) is not used.

Maintenance (60)

Maintenance (60) is not used.

Maintenance (61)

Table 7-59 lists the details of the Maintenance (61) critical alarm. To troubleshoot and correct the cause of the alarm, refer to the "No Heartbeat Messages Received Through the Interface—Maintenance (61)" section on page 7-107.

Table 7-59 Maintenance (61) Details

Description	No Heartbeat Messages Received Through the Interface (No HB Messages Received Through the Interface)
Severity	Critical
Threshold	100
Throttle	0
Datawords	Interface Name—STRING [20] Interface IP Address—STRING [50]
Primary Cause	The local network interface is down.
Primary Action	Restore the local network interface.
Secondary Cause	The mate network interface on the same subnet is faulty.
Secondary Action	Restore the mate network interface.
Ternary Cause	Network congestion.

Maintenance (62)

Table 7-60 lists the details of the Maintenance (62) major alarm. To troubleshoot and correct the cause of the alarm, refer to the "Link Monitor: Interface Lost Communication—Maintenance (62)" section on page 7-107.

Table 7-60 Maintenance (62) Details

Description	Link Monitor: Interface Lost Communication
Severity	Major
Threshold	100
Throttle	0
Datawords	Interface Name—STRING [80] Interface IP Address—STRING [80]
Primary Cause	The interface cable is pulled out or the interface is shut down using **ifconfig down** command.
Primary Action	Restore the network interface.
Secondary Cause	The interface has no connectivity to any of the machines or routers.

Maintenance (63)

Table 7-61 lists the details of the Maintenance (63) major alarm. To troubleshoot and correct the cause of the alarm, refer to the "Outgoing Heartbeat Period Exceeded Limit—Maintenance (63)" section on page 7-108.

Table 7-61 Maintenance (63) Details

Description	Outgoing Heartbeat Period Exceeded Limit (Outgoing HB Period Exceeded Limit)
Severity	Major
Threshold	100
Throttle	0
Datawords	Maximum 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 by using the HMN CLI commands. Verify if this is a persistent situation. Contact Cisco TAC with the gathered information.

Maintenance (64)

Table 7-62 lists the details of the Maintenance (64) major alarm. 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 7-108.

Table 7-62 Maintenance (64) Details

Description	Average Outgoing Heartbeat Period Exceeds Major Alarm Limit (Average Outgoing HB Period Exceeds Maj Alarm Limit)
Severity	Major
Threshold	100
Throttle	0
Datawords	Maximum Avg HB Period—FOUR_BYTES Average 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 by using the HMN CLI commands. Verify if this is a persistent situation. Contact Cisco TAC with the gathered information.

Maintenance (65)

Table 7-63 lists the details of the Maintenance (65) critical alarm. To troubleshoot and correct the cause of the alarm, refer to the "Disk Partition Critically Consumed—Maintenance (65)" section on page 7-108.

Table 7-63 Maintenance (65) Details

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 are writing extraneous data to the named partition.
Primary Action	Perform disk a cleanup and maintenance on the offending system.

Maintenance (66)

Table 7-64 lists the details of the Maintenance (66) major alarm. To troubleshoot and correct the cause of the alarm, refer to the "Disk Partition Significantly Consumed—Maintenance (66)" section on page 7-108.

Table 7-64 Maintenance (66) Details

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 a disk clean-up and maintenance on the offending system.

Maintenance (67)

Table 7-65 lists the details of the Maintenance (67) minor alarm. 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 7-108.

Table 7-65 Maintenance (67) Details

Description	The Free Inter-Process Communication Pool Buffers Below Minor Threshold (The Free IPC Pool Buffers Below Minor Threshold)
Severity	Minor
Threshold	100
Throttle	0
Datawords	Free IPC Pool Buffer—STRING [10] Threshold—STRING [10]
Primary Cause	The IPC pool buffers are not being properly freed 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)

Table 7-66 lists the details of the Maintenance (68) major alarm. 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 7-109.

Table 7-66 Maintenance (68) Details

Description	The Free Inter-Process Communication Pool Buffers Below Major Threshold (The Free IPC Pool Buffers Below Major Threshold)
Severity	Major
Threshold	100
Throttle	0
Datawords	Free IPC Poll Buffer—STRING [10] Threshold—STRING [10]
Primary Cause	Inter-process communication (IPC) pool buffers are not being properly freed 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 (69)

Table 7-67 lists the details of the Maintenance (69) critical alarm. 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 7-109.

Table 7-67 Maintenance (69) Details

Description	The Free Inter-Process Communication Pool Buffers Below Critical Threshold (The Free IPC Pool Buffers Below Critical Threshold)
Severity	Critical
Threshold	100
Throttle	0
Datawords	Free IPC Poll Buffer—STRING [10] Threshold—STRING [10]
Primary Cause	The IPC pool buffers are not being properly freed 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 (70)

Table 7-68 lists the details of the Maintenance (70) critical alarm. 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 7-109.

Table 7-68 Maintenance (70) Details

Description	The Free Inter-Process Communication Pool Buffer Count Below Minimum Required (The Free IPC Pool Buffer Count Below Minimum Required)
Severity	Critical
Threshold	100
Throttle	0
Datawords	Free IPC Buffer Count—TWO_BYTES Minimum Count—TWO_BYTES
Primary Cause	The IPC pool buffers are not being properly freed 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 (71)

Table 7-69 lists the details of the Maintenance (71) major alarm. 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 7-109.

Table 7-69 Maintenance (71) Details

Description	Local Domain Name System Server Response Too Slow (Local DNS Server Response Too Slow)
Severity	Major
Threshold	100
Throttle	0
Datawords	DNS Server IP—STRING [64]
Primary Cause	The local domain name system (DNS) server is too busy.
Primary Action	Check the local DNS server.

Maintenance (72)

Table 7-70 lists the details of the Maintenance (72) major alarm. 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 7-109.

Table 7-70 Maintenance (72) Details

Description	External Domain Name System Server Response Too Slow (External DNS Server Response Too Slow)
Severity	Major
Threshold	100
Throttle	0
Datawords	DNS Server IP—STRING [64]
Primary Cause	The network traffic level is high or the name server is very busy.
Primary Action	Check the DNS server(s).
Secondary Cause	There is a daemon called monitorDNS.sh checking the DNS server every minute or so. It will issue an alarm if it cannot contact the DNS server or the response is slow. But it will clear the alarm if it can contact the DNS server later.

Maintenance (73)

Table 7-71 lists the details of the Maintenance (73) critical alarm. To troubleshoot and correct the cause of the alarm, refer to the "External Domain Name System Server Not Responsive—Maintenance (73)" section on page 7-110.

Table 7-71 Maintenance (73) Details

Description	External Domain Name System Server not Responsive (External DNS Server not Responsive)
Severity	Critical
Threshold	100
Throttle	0
Datawords	DNS Server IP—STRING [64]
Primary Cause	The DNS servers or the network may be down.
Primary Action	Check the DNS server(s).
Secondary Cause	There is a daemon called monitorDNS.sh checking DNS server every minute or so. It will issue an alarm if it cannot contact the DNS server or the response is slow. But it will clear the alarm if it can contact the DNS server later.

Maintenance (74)

Table 7-72 lists the details of the Maintenance (74) critical alarm. To troubleshoot and correct the cause of the alarm, refer to the "Local Domain Name System Service Not Responsive—Maintenance (74)" section on page 7-110.

Table 7-72 Maintenance (74) Details

Description	Local Domain Name System Service not Responsive (Local DNS Service not Responsive)
Severity	Critical
Threshold	100
Throttle	0
Datawords	DNS Server IP—STRING [64] Reason—STRING [64]
Primary Cause	The local DNS service may be down.
Primary Action	Check the local DNS server.

Maintenance (75)

Table 7-73 lists the details of the Maintenance (75) warning event. 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 7-87.

Table 7-73 Maintenance (75) Details

Description	Mismatch of Internet Protocol Address Local Server and Domain Name System (Mismatch of IP Addr% Local Server and DNS)
Severity	Warning
Threshold	100
Throttle	0
Datawords	Host Name—STRING [64] IP Addr Local Server—STRING [64] IP Addr DNS Server—STRING [64]
Primary Cause	The DNS updates are not getting to the Cisco BTS 10200 from the external server or a discrepancy was detected before the local DNS lookup table was updated.
Primary Action	Ensure that the external DNS server is operational and is sending updates to the Cisco BTS 10200.

Maintenance (76)

Maintenance (76) is not used.

Maintenance (77)

Table 7-74 lists the details of the Maintenance (77) major alarm. To troubleshoot and correct the cause of the alarm, refer to the "Mate Time Differs Beyond Tolerance—Maintenance (77)" section on page 7-110.

Table 7-74 Maintenance (77) Details

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 the platform first.

Maintenance (78)

Table 7-75 lists the details of the Maintenance (78) informational event. For additional information, refer to the "Bulk Data Management System Admin State Change—Maintenance (78)" section on page 7-87.

Table 7-75 Maintenance (78) Details

Description	Bulk Data Management System Admin State Change (BDMS Admin State Change)
Severity	Information
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)

Table 7-76 lists the details of the Maintenance (79) informational event. For additional information, refer to the "Resource Reset—Maintenance (79)" section on page 7-87.

Table 7-76 Maintenance (79) Details

Description	Resource Reset
Severity	Information
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)

Table 7-77 lists the details of the Maintenance (80) informational event. For additional information, refer to the "Resource Reset Warning—Maintenance (80)" section on page 7-87.

Table 7-77 Maintenance (80) Details

Description	Resource Reset Warning
Severity	Information
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)

Table 7-78 lists the details of the Maintenance (81) informational event. For additional information, refer to the "Resource Reset Failure—Maintenance (81)" section on page 7-87.

Table 7-78 Maintenance (81) Details

Description	Resource Reset Failure
Severity	Information
Threshold	100
Throttle	0
Datawords	Resource Type—STRING [40] Resource Instance—STRING [40] Failure Reason—STRING [120]
Primary Cause	The informational event is the result of an internal messaging error.
Primary Action	Check Dataword 3 (Failure Reason) to determine if the event was caused by invalid user input, inconsistent provisioning of the device, or if the system is busy and a timeout occurred.

Maintenance (82)

Table 7-79 lists the details of the Maintenance (82) critical alarm. To troubleshoot and correct the cause of the alarm, refer to the "Average Outgoing Heartbeat Period Exceeds Critical Limit—Maintenance (82)" section on page 7-110.

Table 7-79 Maintenance (82) Details

Description	Average Outgoing Heartbeat Period Exceeds Critical Limit (Average Outgoing HB Period Exceeds Critical Limit)
Severity	Critical
Threshold	100
Throttle	0
Datawords	Critical Threshold F—FOUR_BYTES Current Average HB Peri—FOUR_BYTES
Primary Cause	The CPU is overloaded.
Primary Action	Shut down the platform.

Maintenance (83)

Table 7-80 lists the details of the Maintenance (80) minor alarm. To troubleshoot and correct the cause of the alarm, refer to the "Swap Space Below Minor Threshold—Maintenance (83)" section on page 7-110.

Table 7-80 Maintenance (83) Details

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 are running.
Primary Action	Stop the proliferation of executables (process scripts).
Secondary Cause	File spaces /tmp or /var/run are over-used.
Secondary Action	Clean up the file systems.

Maintenance (84)

Table 7-81 lists the details of the Maintenance (84) major alarm. To troubleshoot and correct the cause of the alarm, refer to the "Swap Space Below Major Threshold—Maintenance (84)" section on page 7-110.

Table 7-81 Maintenance (84) Details

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 are running.
Primary Action	Stop the proliferation of executables (process and shell procedures).
Secondary Cause	File spaces /tmp or /var/run are over-used.
Secondary Action	Clean up the file systems.

Maintenance (85)

Table 7-82 lists the details of the Maintenance (85) critical alarm. To troubleshoot and correct the cause of the alarm, refer to the "Swap Space Below Critical Threshold—Maintenance (85)" section on page 7-111.

Table 7-82 Maintenance (85) Details

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 are running.
Primary Action	Restart the Cisco BTS 10200 software or reboot the system.
Secondary Cause	File spaces /tmp or /var/run are over-used.
Secondary Action	Clean up the file systems.

Maintenance (86)

Table 7-83 lists the details of the Maintenance (86) minor alarm. To troubleshoot and correct the cause of the alarm, refer to the "System Health Report Collection Error—Maintenance (86)" section on page 7-111.

Table 7-83 Maintenance (86) Details

Description	System Health Report Collection Error
Severity	Minor
Threshold	100
Throttle	0
Datawords	ErrString—STRING [64]
Primary Cause	An error occurred during collection of system health report data.
Primary Action	Contact Cisco TAC for support.

Maintenance (87)

Table 7-84 lists the details of the Maintenance (87) major alarm. To troubleshoot and correct the cause of the alarm, refer to the "Status Update Process Request Failed—Maintenance (87)" section on page 7-111.

Table 7-84 Maintenance (87) Details

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 is not working properly.
Primary Action	Use CLI to verify that the **status** command is working properly.

Maintenance (88)

Table 7-85 lists the details of the Maintenance (88) major alarm. To troubleshoot and correct the cause of the alarm, refer to the "Status Update Process Database List Retrieval Error—Maintenance (88)" section on page 7-111.

Table 7-85 Maintenance (88) Details

Description	Status Update Process Database List Retrieval Error (Status Update Process DB List Retrieval Error)
Severity	Major
Threshold	100
Throttle	0
Datawords	ErrString—STRING [64]
Primary Cause	The Oracle database (DB) is not working properly.
Primary Action	Contact Cisco TAC for support.

Maintenance (89)

Table 7-86 lists the details of the Maintenance (89) major alarm. To troubleshoot and correct the cause of the alarm, refer to the "Status Update Process Database Update Error—Maintenance (89)" section on page 7-111.

Table 7-86 Maintenance (89) Details

Description	Status Update Process Database Update Error (Status Update Process DB Update Error)
Severity	Major
Threshold	100
Throttle	0
Datawords	ErrString—STRING [64] SQL Command—STRING [64]
Primary Cause	The MySQL DB on the EMS is not working properly.
Primary Action	Contact Cisco TAC for support.

Maintenance (90)

Table 7-87 lists the details of the Maintenance (90) minor alarm. To troubleshoot and correct the cause of the alarm, refer to the "Disk Partition Moderately Consumed—Maintenance (90)" section on page 7-111.

Table 7-87 Maintenance (90) Details

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 are writing extraneous data to the named partition.
Primary Action	Perform disk clean-up and maintenance on the offending system.

Maintenance (91)

Table 7-88 lists the details of the Maintenance (91) critical alarm. To troubleshoot and correct the cause of the alarm, refer to the "Internet Protocol Manager Configuration File Error—Maintenance (91)" section on page 7-111.

Table 7-88 Maintenance (91) Details

Description	Internet Protocol Manager Configuration File Error (IPM Config File Error)
Severity	Critical
Threshold	100
Throttle	0
Datawords	Reason—STRING [128]
Primary Cause	The Internet Protocol Manager (IPM) has a configuration file error.
Primary Action	Check the IPM configuration file (ipm.cfg) for incorrect syntax.

Maintenance (92)

Table 7-89 lists the details of the Maintenance (92) major alarm. To troubleshoot and correct the cause of the alarm, refer to the "Internet Protocol Manager Initialization Error—Maintenance (92)" section on page 7-112.

Table 7-89 Maintenance (92) Details

Description	Internet Protocol Manager Initialization Error (IPM Initialization Error)
Severity	Major
Threshold	100
Throttle	0
Datawords	Reason—STRING [128]
Primary Cause	The IPM failed to initialize correctly.
Primary Action	Check the Reason dataword as to the cause of the error.

Maintenance (93)

Table 7-90 lists the details of the Maintenance (93) major alarm. To troubleshoot and correct the cause of the alarm, refer to the "Internet Protocol Manager Interface Failure—Maintenance (93)" section on page 7-112.

Table 7-90 Maintenance (93) Details

Description	Internet Protocol Manager Interface Failure (IPM Interface Failure)
Severity	Major
Threshold	100
Throttle	0
Datawords	Interface Name—STRING [32] Reason—STRING [128]
Primary Cause	The IPM failed to create logical interface.
Primary Action	Check the Reason dataword as to the cause of the error.

Maintenance (94)

Table 7-91 lists the details of the Maintenance (94) informational event. For additional information, refer to the "Internet Protocol Manager Interface State Change—Maintenance (94)" section on page 7-89.

Table 7-91 Maintenance (94) Details

Description	Internet Protocol Manager Interface State Change (IPM Interface State Change)
Severity	Information
Threshold	100
Throttle	0
Datawords	Interface Name—STRING [32] State—STRING [16]
Primary Cause	The IPM changed state on an interface (up/down).
Primary Action	None

Maintenance (95)

Table 7-92 lists the details of the Maintenance (95) informational event. For additional information, refer to the "Internet Protocol Manager Interface Created—Maintenance (95)" section on page 7-90.

Table 7-92 Maintenance (95) Details

Description	Internet Protocol Manager Interface Created (IPM Interface Created)
Severity	Information
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	The IPM created a new logical interface.
Primary Action	None

Maintenance (96)

Table 7-93 lists the details of the Maintenance (96) informational event. For additional information, refer to the "Internet Protocol Manager Interface Removed—Maintenance (96)" section on page 7-90.

Table 7-93 Maintenance (96) Details

Description	Internet Protocol Manager Interface Removed (IPM Interface Removed)
Severity	Information
Threshold	100
Throttle	0
Datawords	Hostname—STRING [128] Logical IF Name—STRING [32] IP Addr—STRING [32]
Primary Cause	The IPM removed a logical interface.
Primary Action	None

Maintenance (97)

Table 7-94 lists the details of the Maintenance (97) critical alarm. 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 7-112.

Table 7-94 Maintenance (97) Details

Description	Inter-Process Communication Input Queue Entered Throttle State (IPC Input Queue Entered Throttle State)
Severity	Critical
Threshold	500
Throttle	0
Datawords	Process Name—STRING [10] 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.

Maintenance (98)

Table 7-95 lists the details of the Maintenance (98) minor alarm. 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 7-112.

Table 7-95 Maintenance (98) Details

Description	Inter-Process Communication Input Queue Depth at 25% of Its Hi-Watermark (IPC Input Queue Depth at 25% of Its Hi-Watermark)
Severity	Minor
Threshold	500
Throttle	0
Datawords	Process Name—STRING [10] 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.

Maintenance (99)

Table 7-96 lists the details of the Maintenance (99) major alarm. 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 7-112.

Table 7-96 Maintenance (99) Details

Description	Inter-Process Communication Input Queue Depth at 50% of Its Hi-Watermark (IPC Input Queue Depth at 50% of Its Hi-Watermark)
Severity	Major
Threshold	500
Throttle	0
Datawords	Process Name—STRING [10] 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.

Maintenance (100)

Table 7-97 lists the details of the Maintenance (100) critical alarm. 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 7-113.

Table 7-97 Maintenance (100) Details

Description	Inter-Process Communication Input Queue Depth at 75% of Its Hi-Watermark (IPC Input Queue Depth at 75% of Its Hi-Watermark)
Severity	Critical
Threshold	500
Throttle	0
Datawords	Process Name—STRING [10] 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.

Maintenance (101)

Table 7-98 lists the details of the Maintenance (101) critical alarm. To troubleshoot and correct the cause of the alarm, refer to the "Switchover in Progress—Maintenance (101)" section on page 7-113.

Table 7-98 Maintenance (101) Details

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 a system switchover occurs either due to a manual switchover (through a CLI command), failover, or automatic switchover.
Primary Action	No action needs to be taken; the alarm is cleared when the switchover is complete. The service is temporarily suspended for a short period of time during this transition.

Maintenance (102)

Table 7-99 lists the details of the Maintenance (102) critical alarm. 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 7-113.

Table 7-99 Maintenance (102) Details

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	A software error has occurred.
Primary Action	None, the system will automatically recover or shut down.

Maintenance (103)

Table 7-100 lists the details of the Maintenance (103) critical alarm. To troubleshoot and correct the cause of the alarm, refer to the "Central Processing Unit Is Offline—Maintenance (103)" section on page 7-113.

Table 7-100 Maintenance (103) Details

Description	Central Processing Unit is Offline (CPU Is Offline)
Severity	Critical
Threshold	100
Throttle	0
Datawords	Hostname—STRING [20] CPU—ONE_BYTE
Primary Cause	An operator action has caused the CPU to go offline.
Primary Action	Restore the CPU or contact Cisco TAC.

Maintenance (104)

Table 7-101 lists the details of the Maintenance (104) informational event. For additional information, refer to the "Aggregration Device Address Successfully Resolved—Maintenance (104)" section on page 7-91.

Table 7-101 Maintenance (104) Details

Description	Aggregration Device Address Successfully Resolved
Severity	Information
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	The event is informational.
Primary Action	No action needs to be taken.

Maintenance (105)

Maintenance (105) is not used.

Maintenance (106)

Maintenance (106) is not used.

Maintenance (107)

Table 7-102 lists the details of the Maintenance (107) critical alarm. 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 7-113.

Table 7-102 Maintenance (107) Details

Description	No Heartbeat Messages Received Through Interface From Router (No HB 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	The router is down.
Primary Action	Restore the router functionality.
Secondary Cause	Connection to the router is down.
Secondary Action	Restore the connection.
Ternary Cause	Network congestion.

Maintenance (108)

Table 7-103 lists the details of the Maintenance (108) warning event. To monitor and correct the cause of the event, refer to the "A Log File Cannot Be Transferred—Maintenance (108)" section on page 7-92.

Table 7-103 Maintenance (108) Details

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	A problem in access to the external archive system has occurred.
Primary Action	Check the external archive system.
Secondary Cause	The network to the 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)

Table 7-104 lists the details of the Maintenance (109) major alarm. To troubleshoot and correct the cause of the alarm, refer to the "Five Successive Log Files Cannot Be Transferred—Maintenance (109)" section on page 7-114.

Table 7-104 Maintenance (109) Details

Description	Five Successive Log Files Cannot Be Transferred
Severity	Major
Threshold	100
Throttle	0
Datawords	External Archive Systems—STRING [100]
Primary Cause	A problem in access to external archive system has occurred.
Primary Action	Check the external archive system.
Secondary Cause	Network to the external archive system is down.
Secondary Action	Check the network.

Maintenance (110)

Table 7-105 lists the details of the Maintenance (110) major alarm. 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 7-114.

Table 7-105 Maintenance (110) Details

Description	Access to Log Archive Facility Configuration File Failed or File Corrupted (Access to LAF Configuration File Failed or File Corrupted)
Severity	Major
Threshold	10
Throttle	0
Datawords	Full Path of LAF Configuration F—STRING [50]
Primary Cause	The LAF file is 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)

Table 7-106 lists the details of the Maintenance (111) critical alarm. To troubleshoot and correct the cause of the alarm, refer to the "Cannot Log In to External Archive Server—Maintenance (111)" section on page 7-114.

Table 7-106 Maintenance (111) Details

Description	Cannot Log In 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 the external archive server for the user from the Cisco BTS 10200.
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.

Maintenance (112)

Table 7-107 lists the details of the Maintenance (112) major alarm. To troubleshoot and correct the cause of the alarm, refer to the "Congestion Status—Maintenance (112)" section on page 7-114.

Table 7-107 Maintenance (112) Details

Description	Congestion Status
Severity	Major
Threshold	100
Throttle	0
Datawords	System MCL Level—ONE_BYTE
Primary Cause	A change has occurred in the system overload level.
Primary Action	If the reported level remains continuously high, adjust the system load or configuration.

Maintenance (113)

Table 7-108 lists the details of the Maintenance (113) informational event. For additional information, refer to the "Central Processing Unit Load of Critical Processes—Maintenance (113)" section on page 7-92.

Table 7-108 Maintenance (113) Details

Description	Central Processing Unit Load of Critical Processes (CPU Load of Critical Processes)
Severity	Information
Threshold	100
Throttle	0
Datawords	Factor Level—ONE_BYTE Factor MCL—ONE_BYTE
Primary Cause	A change (increase/decrease) has occurred in the call processing load.
Primary Action	If the level remains continuously high, change the configuration or redistribute the call load.

Maintenance (114)

Table 7-109 lists the details of the Maintenance (114) informational event. For additional information, refer to the "Queue Length of Critical Processes—Maintenance (114)" section on page 7-93.

Table 7-109 Maintenance (114) Details

Description	Queue Length of Critical Processes
Severity	Information
Threshold	100
Throttle	0
Datawords	Process Name—STRING [5] Factor Level—ONE_BYTE Factor MCL—ONE_BYTE
Primary Cause	A change has occurred in the queue length of the critical processes.
Primary Action	If the reported level remains continuously high, adjust the system load or configuration.

Maintenance (115)

Table 7-110 lists the details of the Maintenance (115) informational event. For additional information, refer to the "Inter-Process Communication Buffer Usage Level—Maintenance (115)" section on page 7-93.

Table 7-110 Maintenance (115) Details

Description	Inter-Process Communication Buffer Usage Level (IPC Buffer Usage Level)
Severity	Information
Threshold	100
Throttle	0
Datawords	Factor Level—ONE_BYTE Factor MCL—ONE_BYTE
Primary Cause	A change has occurred in the IPC buffer usage.
Primary Action	If the reported level remains continuously high, adjust the system load or configuration.

Maintenance (116)

Table 7-111 lists the details of the Maintenance (116) informational event. For additional information, refer to the "Call Agent Reports the Congestion Level of Feature Server—Maintenance (116)" section on page 7-93.

Table 7-111 Maintenance (116) Details

Description	Call Agent Reports the Congestion Level of the Feature Server (CA Reports the Congestion Level of FS)
Severity	Information
Threshold	100
Throttle	0
Datawords	Domain Name of FS—STRING [65] Feature Server ID—STRING [20]
Primary Cause	The Feature Server is congested.
Primary Action	No action is required.

Maintenance (117)

Table 7-112 lists the details of the Maintenance (117) critical alarm. To troubleshoot and correct the cause of the alarm, refer to the "Side Automatically Restarting Due to Fault—Maintenance (117)" section on page 7-114.

Table 7-112 Maintenance (117) Details

Description	Side Automatically Restarting Due to Fault
Severity	Critical
Threshold	100
Throttle	0
Datawords	Time of next restart attempt—STRING [25]
Primary Cause	The platform has shut down due to the OOS-FAULTY state, and is in the process of being automatically restarted.
Primary Action	Capture the debugging information, especially from the saved.debug directory. This alarm indicates that an automatic restart is pending and at what time it will be attempted.

Maintenance (118)

Table 7-113 lists the details of the Maintenance (118) critical alarm. 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 7-115.

Table 7-113 Maintenance (118) Details

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)

Table 7-114 lists the details of the Maintenance (119) critical alarm. To troubleshoot and correct the cause of the alarm, refer to the "Periodic Shared Memory Database Back Up Failure—Maintenance (119)" section on page 115.

Table 7-114 Maintenance (119) Details

Description	Periodic Shared Memory Database Back Up 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)

Table 7-115 lists the details of the Maintenance (120) informational event. For additional information, refer to the "Periodic Shared Memory Database Back Up Success—Maintenance (120)" section on page 94.

Table 7-115 Maintenance (120) Details

Description	Periodic Shared Memory Database Back Up Success
Severity	Information
Threshold	100
Throttle	0
Datawords	Details—STRING [300]
Primary Cause	Successful back up of the shared memory database.
Primary Action	Not applicable.

Maintenance (121)

Table 7-116 lists the details of the Maintenance (121) informational event. For additional information, refer to the "Invalid SOAP Request—Maintenance (121)" section on page 94.

Table 7-116 Maintenance (121) Details

Description	Invalid SOAP Request
Severity	Information
Threshold	100
Throttle	0
Datawords	Request—STRING [256] Session ID—STRING [20]
Primary Cause	The provisioning client sent an invalid xml request to the soap provisioning adapter.
Primary Action	Resend a valid xml request.

Maintenance (122)

Table 7-117 lists the details of the Maintenance (122) informational event. For additional information, refer to the "Northbound Provisioning Message Is Retransmitted—Maintenance (122)" section on page 94.

Table 7-117 Maintenance (122) Details

Description	Northbound Provisioning Message Is Retransmitted
Severity	Information
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 may be responding slowly.
Primary Action	Check to see if there are any hub alarms. Take the appropriate action according to the alarms.

Maintenance (123)

Table 7-118 lists the details of the Maintenance (120) warning event. 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 94.

Table 7-118 Maintenance (123) Details

Description	Northbound Provisioning Message Dropped Due To Full Index Table (Northbound Provisioning Message Dropped Due To Full IDX 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.

Maintenance (124)

Table 7-119 lists the details of the Maintenance (124) informational event. For additional information, refer to the "Periodic Shared Memory Sync Started—Maintenance (124)" section on page 7-94.

Table 7-119 Maintenance (124) Details

Description	Periodic Shared Memory Sync Started
Severity	Information
Threshold	100
Throttle	0
Primary Cause	Serves as an information alert that a periodic shared-memory synchronization has successfully started on the Cisco BTS 10200 system.
Primary Action	The customer should monitor the Cisco BTS 10200 system for the successful completion of the periodic shared-memory synchronization as indicated by the Periodic Shared Memory Sync Completed event.

Maintenance (125)

Table 7-120 lists the details of the Maintenance (125) informational event. For additional information, refer to the "Periodic Shared Memory Sync Completed—Maintenance (125)" section on page 7-94.

Table 7-120 Maintenance (125) Details

Description	Periodic Shared Memory Sync Completed
Severity	Information
Threshold	100
Throttle	0
Primary Cause	Serves as an informational alert that a periodic shared-memory synchronization to disk has been successfully completed.
Primary Action	No customer action is required when the periodic shared-memory synchronization is successfully completed by the Cisco BTS 10200 system.

Maintenance (126)

Table 7-121 lists the details of the Maintenance (126) critical alarm. To troubleshoot and correct the cause of the alarm, refer to the "Periodic Shared Memory Sync Failure—Maintenance (126)" section on page 7-115.

Table 7-121 Maintenance (126) Details

Description	Periodic Shared Memory Sync Failure
Severity	Critical
Threshold	100
Throttle	0
Datawords	Failure Details - STRING [300]
Primary Cause	Indicates that the periodic shared-memory synchronization write to disk has failed.
Primary Action	Check the Cisco BTS 10200 system for the cause of the failure, correct it, and then verify that the next periodic shared-memory synchronization to disk is successfully completed by monitoring the Cisco BTS 10200 system for a Periodic Shared Memory Sync Completed informational event

Maintenance (127)

Table 7-122 lists the details of the Maintenence (127) critical alarm. To troubleshoot and correct the cause of the alarm, refer to the "Manual Recovery of OMS HUB Queue Loss—Maintenance (127)" section on page 7-115.

Table 7-122 Maintenance (127) Details

Description	Loss in OMS Hub Communication
Severity	Critical
Threshold	100
Throttle	0
Dataword	Queue-Name - STRING[8] Platform - STRING[8] Node - STRING[8]
Primary Cause	Indicates either a network problem or socket connection causing OMS queue loss.
Primary Action	Manually restart the OMS and SMG processes. Refer section Manual Recovery of OMS HUB Queue Loss—Maintenance (127).

Monitoring Maintenance Events

This section provides the information you need for monitoring and correcting maintenance events. Table 7-123 lists all of the maintenance events in numerical order and provides cross-references to each subsection.

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

Table 7-123 Cisco BTS 10200 Maintenance Events

Event Type	Event Name	Event Severity
Maintenance (1)	Test Report—Maintenance (1)	Information
Maintenance (2)	Report Threshold Exceeded—Maintenance (2)	Information
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)	Information
Maintenance (12)	Initialization Successful—Maintenance (12)	Information
Maintenance (13)	Administrative State Change—Maintenance (13)	Information
Maintenance (14)	Call Agent Administrative State Change—Maintenance (14)	Information
Maintenance (15)	Feature Server Administrative State Change—Maintenance (15)	Information
Maintenance (16)	Process Manager: Process Has Died: Starting Process—Maintenance (16)	Information
Maintenance (17)	Invalid Event Report Received—Maintenance (17)	Information
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)	Information
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)	Information

Table 7-123 Cisco BTS 10200 Maintenance Events (continued)

Event Type	Event Name	Event Severity
Maintenance (26)	Process Manager: Going Faulty—Maintenance (26)	Major
Maintenance (27)	Process Manager: Changing Over to Active—Maintenance (27)	Information
Maintenance (28)	Process Manager: Changing Over to Standby—Maintenance (28)	Information
Maintenance (29)	Administrative State Change Failure—Maintenance (29)	Warning
Maintenance (30)	Element Manager State Change—Maintenance (30)	Information
Maintenance (32)	Process Manager: Sending Go Active to Process—Maintenance (32)	Information
Maintenance (33)	Process Manager: Sending Go Standby to Process—Maintenance (33)	Information
Maintenance (34)	Process Manager: Sending End Process to Process—Maintenance (34)	Information
Maintenance (35)	Process Manager: All Processes Completed Initialization—Maintenance (35)	Information
Maintenance (36)	Process Manager: Sending All Processes Initialization Complete to Process—Maintenance (36)	Information
Maintenance (37)	Process Manager: Killing Process—Maintenance (37)	Information
Maintenance (38)	Process Manager: Clearing the Database—Maintenance (38)	Information
Maintenance (39)	Process Manager: Cleared the Database—Maintenance (39)	Information
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)	Information
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

Table 7-123 Cisco BTS 10200 Maintenance Events (continued)

Event Type	Event Name	Event Severity
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)	Information
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)	Information
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)	Information
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)	Information
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
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

Table 7-123 Cisco BTS 10200 Maintenance Events (continued)

Event Type	Event Name	Event Severity
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)	Information
Maintenance (79)	Resource Reset—Maintenance (79)	Information
Maintenance (80)	Resource Reset Warning—Maintenance (80)	Information
Maintenance (81)	Resource Reset Failure—Maintenance (81)	Information
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)	Information
Maintenance (95)	Internet Protocol Manager Interface Created—Maintenance (95)	Information
Maintenance (96)	Internet Protocol Manager Interface Removed—Maintenance (96)	Information
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

Table 7-123 Cisco BTS 10200 Maintenance Events (continued)

Event Type	Event Name	Event Severity
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)	Information
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 Log In to External Archive Server—Maintenance (111)	Critical
Maintenance (112)	Congestion Status—Maintenance (112)	Major
Maintenance (113)	Central Processing Unit Load of Critical Processes—Maintenance (113)	Information
Maintenance (114)	Queue Length of Critical Processes—Maintenance (114)	Information
Maintenance (115)	Inter-Process Communication Buffer Usage Level—Maintenance (115)	Information
Maintenance (116)	Call Agent Reports the Congestion Level of Feature Server—Maintenance (116)	Information
Maintenance (117)	Side Automatically Restarting Due to Fault—Maintenance (117)	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 Back Up Failure—Maintenance (119)	Critical
Maintenance (120)	Periodic Shared Memory Database Back Up Success—Maintenance (120)	Information
Maintenance (121)	Invalid SOAP Request—Maintenance (121)	Information
Maintenance (122)	Northbound Provisioning Message Is Retransmitted—Maintenance (122)	Information
Maintenance (123)	Northbound Provisioning Message Dropped Due to Full Index Table—Maintenance (123)	Warning
Maintenance (124)	Periodic Shared Memory Sync Started—Maintenance (124)	Information
Maintenance (125)	Periodic Shared Memory Sync Completed—Maintenance (125)	Information

Table 7-123 Cisco BTS 10200 Maintenance Events (continued)

Event Type	Event Name	Event Severity
Maintenance (126)	Periodic Shared Memory Sync Failure—Maintenance (126)	Critical
Maintenance (127)	Manual Recovery of OMS HUB Queue Loss—Maintenance (127)	Critical

Test Report—Maintenance (1)

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

Report Threshold Exceeded—Maintenance (2)

The Report Threshold Exceeded event functions as an informational alert that a report threshold has been exceeded. The primary cause of the event is that the threshold for a given report type and number has been exceeded. No further action is required since this is an information report. The Root Cause event report threshold should be investigated to determine if there is a service-affecting situation.

Local Side Has Become Faulty—Maintenance (3)

The Local Side Has Become Faulty alarm (major) indicates that the local side has become faulty. To troubleshoot and correct the cause of the Local Side Has Become Faulty alarm, refer to the "Local Side Has Become Faulty—Maintenance (3)" section on page 7-99.

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 7-99.

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 7-99.

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 7-100.

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 7-100.

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 7-103.

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 7-103.

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 7-103.

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: Process Has Died: 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 is issued prior to the database initialization, these events are informational and can be ignored; otherwise, contact Cisco TAC.

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 7-103.

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 7-103.

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 7-104.

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 7-104.

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 troubleshoot 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 7-104.

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 7-104.

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 7-104.

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 through a 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. Analyze the cause of the failure if you can find one. Verify that the controlling element of the targeted device was in the active state in order to change the adminstrator 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 through a 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 having 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 having 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. 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 7-105.

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 the number of heartbeat (HB) messages being received is less than 50% of the 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 7-105.

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 7-105.

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 7-105.

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 7-105.

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 7-105.

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 7-106.

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 7-106.

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 7-106.

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 7-106.

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 7-106.

The Central Processing Unit Has Returned to Normal Levels of Operation—Maintenance (54)

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 7-107.

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 Cisco 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 7-107.

Memory and Swap Are Consumed at Abnormal Levels—Maintenance (58)

Note Maintenance (58) is issued by the Cisco 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 that 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 they are, only lightening the effective load on the system will clear the situation. If some subsystems are not performing normally, verify which process(es) are running at abnormally high rates, and contact Cisco TAC.

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 7-107.

Link Monitor: Interface Lost Communication—Maintenance (62)

The Link Monitor: Interface Lost Communication alarm (major) indicates that an 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 7-107.

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 7-108.

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 7-108.

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 7-108.

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 7-108.

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 7-108.

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 7-109.

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 7-109.

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 7-109.

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 7-109.

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 7-109.

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 7-110.

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 7-110.

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 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.

Mate Time Differs Beyond Tolerance—Maintenance (77)

The Mate Time Differs Beyond Tolerance alarm (major) indicates that the mate time 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 7-110.

Bulk Data Management System Admin State Change—Maintenance (78)

The Bulk Data Management System Admin State Change event functions as an informational alert that the BDMS administrative state has changed. The primary cause of the event is that the Bulk Data Management Server was switched over manually. The event is informational and no further action is required.

Resource Reset—Maintenance (79)

The Resource Reset event functions as an informational alert that a resource reset has occurred. The event is informational and no further action is required.

Resource Reset Warning—Maintenance (80)

The Resource Reset Warning event functions as an informational alert that a resource reset is about to occur. The event is informational and no further action is required.

Resource Reset Failure—Maintenance (81)

The Resource Reset Failure event functions as an informational alert that a resource reset has failed. The primary cause of the event is an internal messaging error. Check dataword 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.

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 7-110.

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 7-110.

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 7-110.

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 Critical Threshold alarm, refer to the "Swap Space Below Critical Threshold—Maintenance (85)" section on page 7-111.

System Health Report Collection Error—Maintenance (86)

The System Health Report Collection Error alarm (minor) indicates that an error occurred during collection of the 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 7-111.

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 7-111.

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 7-111.

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 7-111.

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 7-111.

Internet Protocol Manager Configuration File Error—Maintenance (91)

The Internet Protocol Manager Configuration File Error alarm (critical) indicates that an 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 7-111.

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 7-112.

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 7-112.

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 7-112.

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 7-112.

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 7-112.

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 7-113.

Switchover in Progress—Maintenance (101)

The Switchover in Progress alarm (critical) indicates that a system switchover is in progress. This alarm is issued when a system switchover is in progress either due to manual switchover (through a 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 system automatically recovers or shutdowns.

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 7-113.

Aggregration Device Address Successfully Resolved—Maintenance (104)

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

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

The No Heartbeat Messages Received Through Interface From Router alarm (critical) indicates that 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 7-113.

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 7-114.

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 7-114.

Cannot Log In to External Archive Server—Maintenance (111)

The Cannot Log In to External Archive Server alarm (critical) indicates that the user cannot log in to the external archive server. To troubleshoot and correct the cause of the Cannot Log In to External Archive Server alarm, refer to the "Cannot Log In to External Archive Server—Maintenance (111)" section on page 7-114.

Congestion Status—Maintenance (112)

The Congestion Status alarm (major) indicates that a change has occurred in the system overload level. To troubleshoot and correct the cause of the Congestion Status alarm, refer to the "Congestion Status—Maintenance (112)" section on page 7-114.

Central Processing Unit Load of Critical Processes—Maintenance (113)

The Central Processing Unit Load of Critical Processes event serves as an informational alert that a change (increase/decrease) has occurred in the call processing load. If the level remains continuously high, change the configuration or redistribute the call load.

Queue Length of Critical Processes—Maintenance (114)

The Queue Length of Critical Processes event serves as an informational alert that a change has occurred in the queue length of critical processes. If the reported level remains continuously high, adjust the system load or configuration.

Inter-Process Communication Buffer Usage Level—Maintenance (115)

The Inter-Process Communication Buffer Usage Level event serves as an informational alert that a change has occurred in the IPC buffer usage. If the reported level remains continuously high, adjust the system load or configuration.

Call Agent Reports the Congestion Level of Feature Server—Maintenance (116)

The Call Agent Reports the Congestion Level of Feature Server event serves as an informational alert that the Feature Server is congested. The event is informational and no further action is required.

Side Automatically Restarting Due to Fault—Maintenance (117)

The Side Automatically Restarting Due to Fault alarm (critical) indicates that the platform has shut down to the OOS-FAULTY state, and is in the process of being automatically restarted. To troubleshoot and correct the cause of the Side Automatically Restarting Due to Fault alarm, refer to the "Side Automatically Restarting Due to Fault—Maintenance (117)" section on page 7-114.

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 7-115.

Periodic Shared Memory Database Back Up Failure—Maintenance (119)

The Periodic Shared Memory Database Back Up Failure alarm (critical) indicates that the periodic shared memory database back up has failed. To troubleshoot and correct the cause of the Periodic Shared Memory Database Back Up Failure alarm, refer to the "Periodic Shared Memory Database Back Up Failure—Maintenance (119)" section on page 7-115.

Periodic Shared Memory Database Back Up Success—Maintenance (120)

The Periodic Shared Memory Database Back Up Success event serves as an informational alert that the periodic shared memory database back up was successfully completed. The event is informational and no further action is required.

Invalid SOAP Request—Maintenance (121)

The Invalid SOAP Request event serves as an informational alert that an invalid SOAP request was issued. The primary cause of the event is that a provisioning client sent an invalid XML request to the SOAP provisioning adapter. To correct the primary cause of the event, resend a valid XML request.

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 an 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 an EMS hub is not responding. To correct the primary cause of the event, find out if there are any alarms originating from the hub and take the appropriate action.

Periodic Shared Memory Sync Started—Maintenance (124)

The Periodic Shared Memory Sync Started event serves as an information alert that a periodic shared-memory synchronization has successfully started on the Cisco BTS 10200 system. The customer should monitor the Cisco BTS 10200 system for the successful completion of the periodic shared-memory synchronization as indicated by the Periodic Shared Memory Sync Completed event.

Periodic Shared Memory Sync Completed—Maintenance (125)

The Periodic Shared Memory Sync Completed event serves as an informational alert that a periodic shared-memory synchronization to disk has been successfully completed. No customer action is required when the periodic shared-memory synchronization is successfully completed by the Cisco BTS 10200 system.

Periodic Shared Memory Sync Failure—Maintenance (126)

The Periodic Shared Memory Sync Failure alarm (critical) indicates that the periodic shared-memory synchronization write to disk has failed. To troubleshoot and correct the cause of the Periodic Shared Memory Sync Failure alarm, check the Cisco BTS 10200 system for the cause of the failure, correct it, and then verify that the next periodic shared-memory synchronization to disk is successfully completed by monitoring the Cisco BTS 10200 system for a Periodic Shared Memory Sync Completed informational event.

Manual Recovery of OMS HUB Queue Loss—Maintenance (127)

The Manual Recovery of OMS HUB Queue Loss alarm (critical) indicates that due to some network or socket connetion issues, the OMS queue is lost causing communication problem between the Cisco BTS 10200 processes. To troubleshoot and correct the cause of the Manual Recovery of OMS HUB Queue Loss alarm, the operator needs to run the manual clean-up procedure such as *pkill smg3* or *pkill hub3* on all the four nodes. It is recommended to perform this task on the maintenance window.

This procedure should be run when critical queues (mentioned below) are lost:

- BULK_OAM—Indicates provisioning queue.
- SCADM—Indicates status or control command queue.
- TMProvision—measurement related changes (used by **measurement_prov** CLI command.)
- QUEUE_THREAD_FSAINxxx—Indicates queue thread for sending AIN provisioning data.
- QUEUE_THREAD_FSPTCxxx—Indicates queue thread for sending PTC provisioning data.
- QUEUE_THREAD_CAxxx—Indicates queue thread for sending CA provisioning data.
- HANDSET_ACK—Indicates handset related queue.
- TrafficGA—Indicates measurement data (from CA to EMS).
- SystemManager—Used for system related command like **block** or **unblock**.

Troubleshooting Maintenance Alarms

This section provides the information you need for troubleshooting and correcting maintenance alarms. Table 7-124 lists all of the maintenance alarms in numerical order and provides cross-references to each subsection.

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

Table 7-124 Cisco BTS 10200 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

Table 7-124 Cisco BTS 10200 Maintenance Alarms (continued)

Alarm Type	Alarm Name	Alarm Severity
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
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

Table 7-124 Cisco BTS 10200 Maintenance Alarms (continued)

Alarm Type	Alarm Name	Alarm Severity
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
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 Log In to External Archive Server—Maintenance (111)	Critical
Maintenance (112)	Congestion Status—Maintenance (112)	Major
Maintenance (117)	Side Automatically Restarting Due to Fault—Maintenance (117)	Critical

Table 7-124 Cisco BTS 10200 Maintenance Alarms (continued)

Alarm Type	Alarm Name	Alarm Severity
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 Back Up Failure—Maintenance (119)	Critical
Maintenance (126)	Periodic Shared Memory Sync Failure—Maintenance (126)	Critical
Maintenance (127)	Manual Recovery of OMS HUB Queue Loss—Maintenance (127)	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 report 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 Cisco BTS 10200 Softswitch CLI Database 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.

Changeover Failure—Maintenance (5)

The Changeover Failure alarm (major) indicates that a changeover failed. The alarm is issued when there is a change 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.

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 change over 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. Restart the platform identified in the alarm report. 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.

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 7-99. 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 retry the **control** command. 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.

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

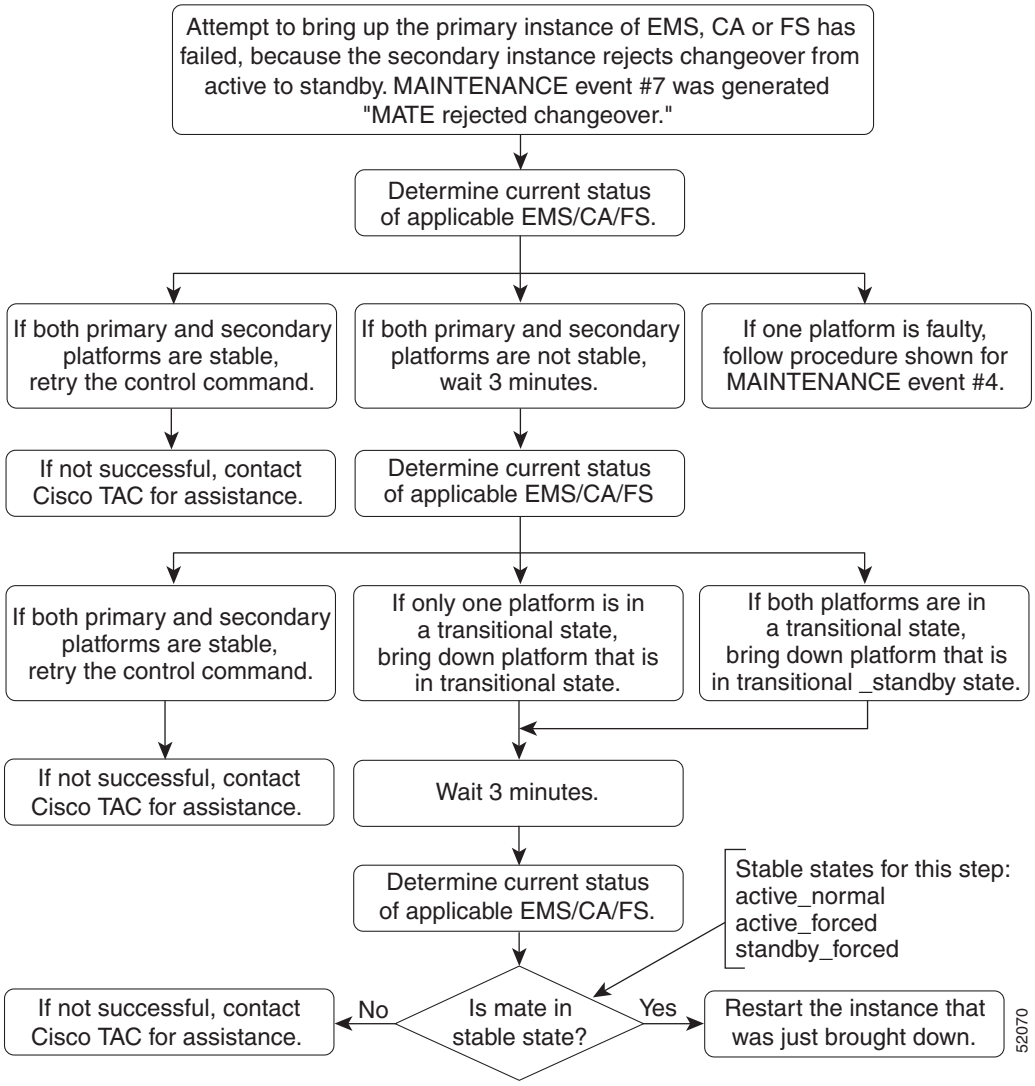
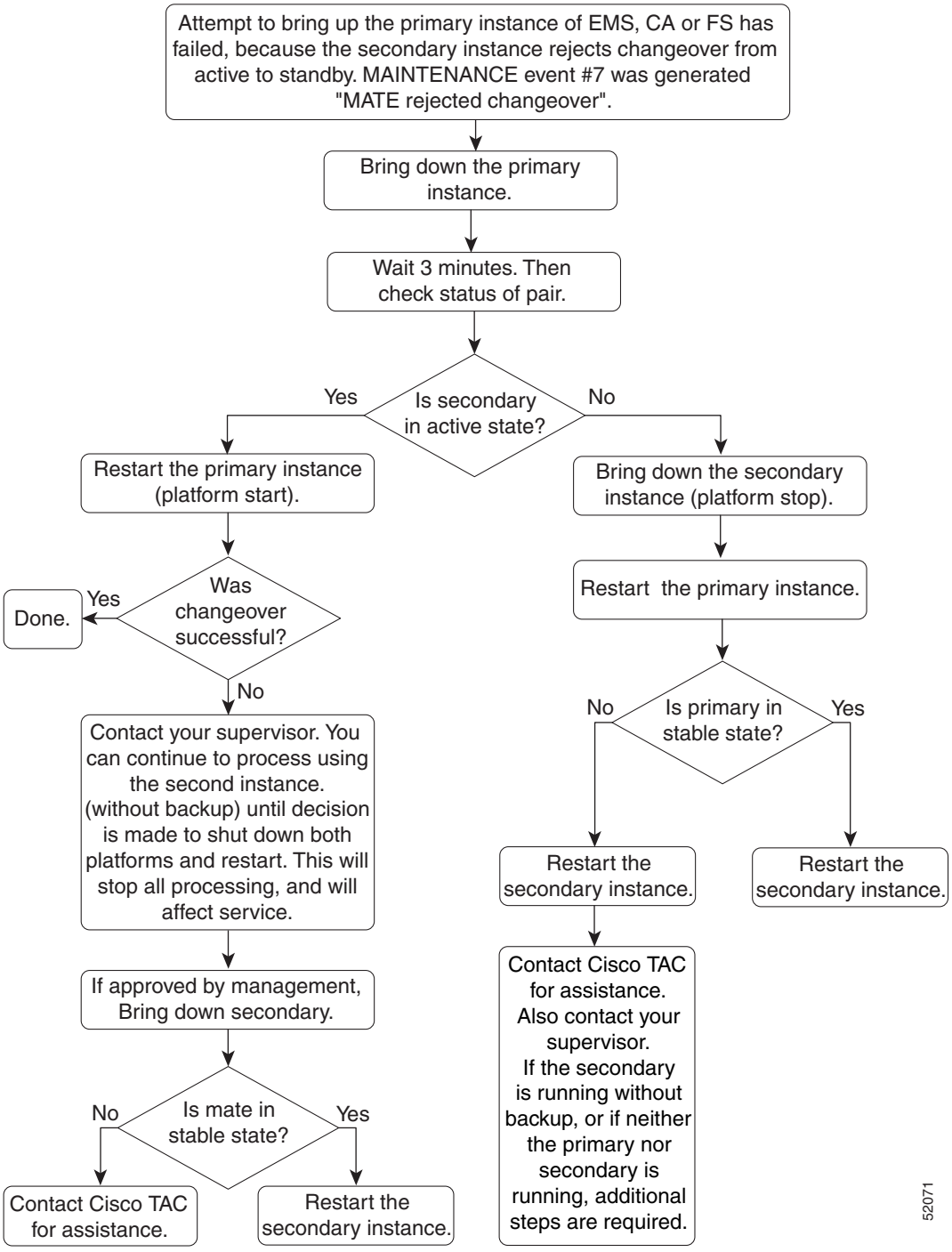


Figure 7-2 Corrective Action for Maintenance Event (7) (Mate Rejected Changeover) Primary Failed To Come Up in Active State



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 reinitialization 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 reinstall the files from the initial or the back up 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 reinitialization 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 reinstall the files from initial or back up 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.

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 from the event and 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 it has, 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 it is not installed, 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.

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 7-99.

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.

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.

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.

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.

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.

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.

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 too numerous to determine. Try to isolate the problem and Call Cisco TAC for assistance.

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.

Memory and Swap Are Consumed at Critical Levels—Maintenance (57)

Note Maintenance (57) is issued by the Cisco 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 they are, only lightening the effective load on the system will clear the situation. If they are not, verify which process(es) are running at abnormally high rates and provide the information to Cisco TAC.

No Heartbeat Messages Received Through the Interface—Maintenance (61)

The No Heartbeat Messages Received Through the Interface alarm (critical) indicates that no HB messages are being received through the local network interface. The primary cause of the alarm is that the local network interface is down. To correct the primary cause of the alarm, restore the local network interface. The secondary cause of the alarm is that the mate network interface on the same sub-net is faulty. To correct the secondary cause of the alarm, restore the mate network interface. The 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 preset 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 through use of the CLI commands to verify if this is a persistent or on-going situation. Contact Cisco TAC with the gathered information.

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 through us of the CLI commands to verify if this is a persistent or on-going situation. Contact Cisco TAC with the gathered information.

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 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.

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.

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.

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.

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 high, 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 a daemon called monitorDNS.sh checking DNS server every minute or so. It will issue alarm if it cannot contact the DNS server or the response is slow. But it will clear the alarm if later it can contact the DNS server.

Local Domain Name System Service Not Responsive—Maintenance (74)

The Local Domain Name System Service Not Responsive alarm (critical) indicates that the local DNS server is not responding to network queries. The primary cause of the alarm is that the local DNS service may be down. To correct the primary cause of the alarm, check the local DNS server.

Mate Time Differs Beyond Tolerance—Maintenance (77)

The Mate Time Differs Beyond Tolerance alarm (major) indicates that the mate differs beyond the tolerance. The primary cause of the alarm is that time synchronization not working. To correct the primary cause of the alarm, change the UNIX time on the faulty or standby side. If the change is occur on the standby, stop platform first.

Average Outgoing Heartbeat Period Exceeds Critical Limit—Maintenance (82)

The Average Outgoing Heartbeat Period Exceeds Critical Limit alarm (critical) indicates that the average outgoing HB period has exceeded the critical limit threshold. The primary cause of the alarm is that the CPU is overloaded. To correct the primary cause of the alarm, shut down 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 is being over-used. To correct the secondary cause of the alarm, clean up 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 is being over-used. To correct the secondary cause of the alarm, clean up 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 software or reboot system The secondary cause of the alarm is that the /tmp or /var/run is being over-used. To correct the secondary cause of the alarm, clean up the file systems.

System Health Report Collection Error—Maintenance (86)

The System Health Report Collection Error alarm (minor) indicates that an error occurred during the collection of date for the System Health Report. The primary cause of the alarm is that an error occurred during the collection of data for the System Health Report. To correct the primary cause of the alarm, contact Cisco TAC.

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, use CLI to verify that the **status** command is working properly.

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.

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.

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 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 a 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.

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.

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.

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.

Switchover in Progress—Maintenance (101)

The Switchover in Progress alarm (critical) indicates that a system switchover is in progress. This alarm is issued when a system switchover is in progress either due to manual switchover (through 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 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.

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

The No Heartbeat Messages Received Through Interface From Router alarm (critical) indicates that 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 Log In to External Archive Server—Maintenance (111)

The Cannot Log In to External Archive Server alarm (critical) indicates that the user cannot log in 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. 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.

Congestion Status—Maintenance (112)

The Congestion Status alarm (major) indicates that a change in the system overload level has occurred. If the reported level remains continuously high, adjust the system load or configuration.

Side Automatically Restarting Due to Fault—Maintenance (117)

The Side Automatically Restarting Due to Fault alarm (critical) indicates that the platform has shut down to the OOS-FAULTY state, and is in the process of being automatically restarted. Additionally, the alarm indicates that an automatic restart is pending and at what time it will be attempted.To troubleshoot and correct the cause of the Side Automatically Restarting Due to Fault alarm, capture the debugging information, especially from the saved.debug directory.

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 Back Up Failure—Maintenance (119)

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

Periodic Shared Memory Sync Failure—Maintenance (126)

The Periodic Shared Memory Sync Failure alarm (critical) indicates that the periodic shared-memory synchronization write to disk has failed. To troubleshoot and correct the cause of the Periodic Shared Memory Sync Failure alarm, check the Cisco BTS 10200 system for the cause of the failure, correct it, and then verify that the next periodic shared-memory synchronization to disk is successfully completed by monitoring the Cisco BTS 10200 system for a Periodic Shared Memory Sync Completed informational event.

Manual Recovery of OMS HUB Queue Loss—Maintenance (127)

The Manual Recovery of OMS HUB Queue Loss alarm (critical) indicates that due to some network or socket connetion issues, the OMS queue is lost causing communication problem between the Cisco BTS 10200 processes. To troubleshoot and correct the cause of the Manual Recovery of OMS HUB Queue Loss alarm, the operator needs to run the manual clean-up procedure such as *pkill smg3* or *pkill hub3* on all the four nodes. It is recommended to perform this task on the maintenance window.

This procedure should be run when critical queues (mentioned below) are lost:

- BULK_OAM—Indicates provisioning queue.
- SCADM—Indicates status or control command queue.
- TMProvision—measurement related changes (used by **measurement_prov** CLI command.)
- QUEUE_THREAD_FSAINxxx—Indicates queue thread for sending AIN provisioning data.
- QUEUE_THREAD_FSPTCxxx—Indicates queue thread for sending PTC provisioning data.
- QUEUE_THREAD_CAxxx—Indicates queue thread for sending CA provisioning data.
- HANDSET_ACK—Indicates handset related queue.
- TrafficGA—Indicates measurement data (from CA to EMS).

- SystemManager—Used for system related command like **block** or **unblock**.

CHAPTER 8

Operations Support System Troubleshooting

Revised: August 10, 2011, OL-25016-01

Introduction

This chapter provides the information needed for monitoring and troubleshooting operations support system (OSS) 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 for monitoring and correcting the operations support system events
- Troubleshooting Operations Support System Alarms—Provides the information needed for troubleshooting and correcting the 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; the event and alarms are arranged in numerical order. Table 8-1 lists all of the operations support system all of the events and alarms by severity.

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

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	Information	Not Used
OSS (23)	OSS (2)	OSS (5)	OSS (7)	OSS (1)	OSS (13)
	OSS (3)	OSS (8)	OSS (11)	OSS (16)	OSS (15)
	OSS (4)	OSS (9)	OSS (12)	OSS (17)	
	OSS (20)	OSS (20)	OSS (24)	OSS (18)	
	OSS (10)			OSS (19)	
	OSS (14)			OSS (21)	
	OSS (22)				

OSS (1)

Table 8-2 lists the of the Operations Support System (1) informational event. For additional information, refer to the "Test Report—Operations Support System (1)" section on page 8-16.

Table 8-2 Operations Support System (1) Details

Description	Test Report
Severity	Information
Threshold	10000
Throttle	0

OSS (2)

Table 8-3 lists the details of the Operations Support System (2) major alarm. To troubleshoot and correct the cause of the alarm, refer to the "Undefined Variable in Known Set—Operations Support System (2)" section on page 8-20.

Table 8-3 Operations Support System (2) Details

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	No definition of a data column could be found in the database.
Primary Action	Contact Cisco Technical Assistance Center (TAC) for support.

OSS (3)

Table 8-4 lists the details of the Operations Support System (3) major alarm. To troubleshoot and correct the cause of the alarm, refer to the "Undefined Data Column Identification—Operations Support System (3)" section on page 8-21.

Table 8-4 Operations Support System (3) Details

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 through the Simple Network Management Protocol (SNMP) interface.
Primary Action	Contact Cisco TAC for support.

OSS (4)

Table 8-5 lists the details of the Operations Support System (4) major alarm. To troubleshoot and correct the cause of the alarm, refer to the "Request Handler Instantiation Error—Operations Support System (4)" section on page 8-21.

Table 8-5 Operations Support System (4) Details

Description	Request Handler Instantiation Error
Severity	Major
Threshold	100
Throttle	0
Datawords	User Name—STRING [40] Host—STRING [40] Subsystem—STRING [64]
Primary Cause	A resource limitation has prevented the creation of this object. This may be caused by a lack of memory or by a class path problem.
Primary Action	Contact Cisco TAC for support.

OSS (5)

Table 8-6 lists the details of the Operations Support System (5) minor alarm. 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 8-21.

Table 8-6 Operations Support System (5) Details

Description	Structured Query Language Error While Getting Statistics (SQL Error While Getting Statistics)
Severity	Minor
Threshold	100
Throttle	0
Datawords	Statistics Category—STRING [40]
Primary Cause	An error occurred in accessing the Structured Query Language (SQL) database for statistical information in the SNMP subsystem. This may be caused by a schema error.
Primary Action	Contact Cisco TAC for support.

OSS (6)

Table 8-7 lists the details of the Operations Support System (6) major alarm. To troubleshoot and correct the cause of the alarm, refer to the "Structured Query Language Connection Error—Operations Support System (6)" section on page 8-21.

Table 8-7 Operations Support System (6) Details

Description	Structured Query Language Connection Error (SQL Connection Error)
Severity	Major
Threshold	100
Throttle	0
Datawords	Error Exception—STRING [64]
Primary Cause	The connection to the database timed out or the database server is not running. This alarm is generated in the SNMP subsystem.
Primary Action	Contact Cisco TAC for support.

OSS (7)

Table 8-8 lists the details of the Operations Support System (7) warning event. 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 8-17.

Table 8-8 Operations Support System (7) Details

Description	Simple Network Management Protocol File Read Error (SNMP File Read Error)
Severity	Warning
Threshold	100
Throttle	0
Datawords	Filename—STRING [40]
Primary Cause	The Management Information Base (MIB) file is missing or locked from access by the SNMP subsystem.
Primary Action	Contact Cisco TAC for support.

OSS (8)

Table 8-9 lists the details of the Operations Support System (8) minor alarm. To troubleshoot and correct the cause of the alarm, refer to the "No Reply Received From Destination—Operations Support System (8)" section on page 8-21.

Table 8-9 Operations Support System (8) Details

Description	No Reply Received from Destination
Severity	Minor
Threshold	100
Throttle	5
Datawords	JMS Queue Name—STRING [40]
Primary Cause	This alarm is 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 (that is, when there are 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.
Secondary Action	If components of the system are in the process of failing or being restored 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.

OSS (9)

Operations Support System (9) is not used.

OSS (10)

Table 8-10 lists the details of the Operations Support System (10) major alarm. 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 8-17.

Table 8-10 Operations Support System (10) Details

Description	Queue Processing Module Database Management Index Failed with Error (QAM DBM IDX Failed with Error)
Severity	Major
Threshold	50
Throttle	0
Datawords	Transaction ID—STRING [32] Sequence Number—EIGHT_BYTES Location Of Error—STRING [16] DBM Result—STRING [64]
Primary Cause	The queue processing module (QAM) is receiving an error because of a 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 the Transaction Queue and execute an Audit on the failed table.
Secondary Cause	The DBM IDX is failing when attempting to perform an **SQL** command.
Secondary Action	Contact Cisco TAC.

OSS (11)

Table 8-11 lists the details of the Operations Support System (11) warning event. 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 8-17.

Table 8-11 Operations Support System (11) Details

Description	Queue Processing Module Database Management Index Mismatch During Add or Delete (QAM DBM IDX mismatch during Add or Delete)
Severity	Warning
Threshold	100
Throttle	0
Datawords	Transaction ID—STRING [32] Sequence Number—EIGHT_BYTES Location Of Error—STRING [16] DBM Result—STRING [64]
Primary Cause	The QAM is received a warning that either an entry already exists in DBM IDX during an add or an entry is nonexistent during a delete operation.
Primary Action	None needed.

OSS (12)

Table 8-12 lists the details of the Operations Support System (12) warning event. To monitor and correct the cause of the event, refer to the "User Session Count Is Approaching Threshold Limit—Operations Support System (12)" section on page 8-18.

Table 8-12 Operations Support System (12) Details

Description	User Session Count is Approaching Threshold Limit
Severity	Warning
Threshold	100
Throttle	0
Datawords	Session Type - STRING [16] Session Maximum Limit - STRING [3] Session Current Usage - STRING [3] Session Usage Percentage - STRING [3]
Primary Cause	The user session usage has reached allowed limit.
Primary Action	Use **report client_session** command to view all log in sessions. Use **stop client_session** to remove stale sessions.

OSS (13)

Operations Support System (13) is not used. It is reserved for future use.

OSS (14)

Table 8-13 lists the details of the Operations Support System (14) major alarm. To troubleshoot and correct the cause of the alarm, refer to the "User Session Count Exceeds Major Threshold Limit—Operations Support System (14)" section on page 8-22.

Table 8-13 Operations Support System (14) Details

Description	User Session Count Exceeds Major Threshold Limit
Severity	Major
Threshold	100
Throttle	0
Datawords	Session Type - STRING [16] Session Maximum Limit - STRING [3] Session Current Usage - STRING [3] Session Usage Percentage - STRING [3]
Primary Cause	The user session usage has reached maximum allowed limit.
Primary Action	Use the **report client_session** command to view all log in sessions. Use the **stop client_session** command to remove stale sessions.

OSS (15)

Operations Support System (15) is not used. It is reserved for future use.

OSS (16)

Table 8-14 lists the details of the Operations Support System (16) informational event. For additional information, refer to the "Session Has Been Removed by Session Control Policy—Operations Support System (16)" section on page 8-18.

Table 8-14 Operations Support System (16) Details

Description	Session Has Been Removed by Session Control Policy
Severity	Information
Threshold	100
Throttle	0
Datawords	Policy ID - STRING [64] Session Type - STRING [16] User ID - STRING [16] Session Key - STRING [20]
Primary Cause	Session has been removed by the session control policy.
Primary Action	This is an informational alert and no corrective action is necessary.

OSS (17)

Table 8-15 lists the details of the Operations Support System (17) informational event. For additional information, refer to the "Session Has Been Removed—Operations Support System (17)" section on page 8-18.

Table 8-15 Operations Support System (17) Details

Description	Session Has Been Removed
Severity	Information
Threshold	100
Throttle	0
Datawords	Session Type - STRING [16] User ID - STRING [16] Session Key - STRING [20]
Primary Cause	The session was removed since it was idle over the timeout limit.

OSS (18)

Table 8-16 lists the details of the Operations Support System (18) informational event. For additional information, refer to the "Invalid Session Request—Operations Support System (18)" section on page 8-18.

Table 8-16 Operations Support System (18) Details

Description	Invalid Session Request
Severity	Information
Threshold	100
Throttle	0
Datawords	User ID - STRING [16] Session Key - STRING [20] Request - STRING [256]
Primary Cause	The noun, verb, or parameters of the **request** command are not valid.
Primary Action	Check and correct the **request** command.

OSS (19)

Table 8-17 lists the details of the Operations Support System (19) informational event. For additional information, refer to the "Interface Is Active and Operational—Operations Support System (19)" section on page 8-18.

Table 8-17 Operations Support System (19) Details

Description	Interface is Active and Operational
Severity	Information
Threshold	100
Throttle	0
Datawords	Session Type - STRING [16]
Primary Cause	The application interface is active and operational.

OSS (20)

Table 8-18 lists the details of the Operations Support System (20) minor alarm. To troubleshoot and correct the cause of the alarm, refer to the "Interface Is Not Started or Is Not Operational—Operations Support System (20)" section on page 8-22.

Table 8-18 Operations Support System (20) Details

Description	Interface is not Started or is not Operational
Severity	Minor
Threshold	100
Throttle	0
Datawords	Session Type - STRING [16]
Primary Cause	The application interface has failed to start or is not operational.
Primary Action	Restart the application interface.

OSS (21)

Table 8-19 lists the details of the Operations Support System (21) informational event. For additional information, refer to the "Resource Reset—Operations Support System (21)" section on page 8-19.

Table 8-19 Operations Support System (21) Details

Description	Resource Reset
Severity	Information
Threshold	100
Throttle	0
Datawords	Resource Type - STRING [40] Resource Instance - STRING [40]
Primary Cause	The resource has been reset.

OSS (22)

Table 8-20 lists the details of the Operations Support System (22) major alarm. To troubleshoot and correct the cause of the alarm, refer to the "One Peer in the Realm Is Out of Contact—Operations Support System (22)" section on page 8-22.

Table 8-20 Operations Support System (22) Details

Description	One Peer in the Realm is Out of Contact
Severity	Major
Threshold	100
Throttle	0
Datawords	Peer Name - STRING [64] Realm Name - STRING [64]
Primary Cause	The communication between the Cisco BTS 10200 EMS system and the Home Subscriber Server (HSS) has experienced a problem or the HSS is experiencing a problem.
Primary Action	Investigate the network and the HSS.

OSS (23)

Table 8-21 lists the details of the Operations Support System (23) critical alarm. To troubleshoot and correct the cause of the alarm, refer to the "All Peers in the Realm Are Out of Contact—Operations Support System (23)" section on page 8-22.

Table 8-21 Operations Support System (23) Details

Description	All Peers in the Realm are Out of Contact
Severity	Critical
Threshold	100
Throttle	0
Datawords	Realm Name - STRING [64]
Primary Cause	The communication between the Cisco BTS 10200 EMS system and the HSS has experienced a problem, the HSS is experiencing a problem, or the network interface of the Cisco BTS 10200 is experiencing a problem.
Primary Action	Investigate the network, the HSS, and the network interface of the EMS.

OSS (24)

Table 8-22 lists the details of the Operations Support System (24) warning event. To monitor and correct the cause of the event, refer to the "User Log In Sessions Have Reached the User Session Limit—Operations Support System (24)" section on page 8-19.

Table 8-22 Operations Support System (24) Details

Description	User Log In Sessions have Reached the User Session Limit
Severity	Warning
Threshold	100
Throttle	0
Datawords	User ID - STRING [16] Adapter Type - STRING [16] Maximum Session Limit - STRING [3] Number of Denials - STRING [7]
Primary Cause	The user log in has been denied because the maximum session limit has been reached.
Primary Action	Use the **show user_session_limit** command to view the user session limit. Use the **change user_session_limit** command to change the user session limit.

OSS (25)

Table 8-23 lists the details of the Operations Support System (25) informational event. For additional information, refer to the "Event Keep Alive Checked—Operations Support System (25)" section on page 8-19.

Table 8-23 Operations Support System (25) Details

Description	Event Keep Alive Checked
Severity	Information
Threshold	100
Throttle	0
Primary Cause	Not an issue if an event or alarm is sent out and received. No action is required if event or alarm is received. If event or alarm is *not* received periodically, then there is an issue with events and alarms or the SNMP system.
Primary Action	If events and alarms are not received capture the SNMP, EVT, EVT2, and OMS logs and restart the SNMP agent.

Monitoring Operations Support System Events

This section provides the information you need for monitoring and correcting operations support system events. Table 8-24 lists all of the operations support system events in numerical order and provides cross-references to each subsection.

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

Table 8-24 Cisco BTS 10200 Operations Support System Events

Event Type	Event Name	Event Severity
OSS (1)	Test Report—Operations Support System (1)	Information
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 (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
OSS (12)	User Session Count Is Approaching Threshold Limit—Operations Support System (12)	Warning
OSS (14)	User Session Count Exceeds Major Threshold Limit—Operations Support System (14)	Major
OSS (16)	Session Has Been Removed by Session Control Policy—Operations Support System (16)	Information
OSS (17)	Session Has Been Removed—Operations Support System (17)	Information
OSS (18)	Invalid Session Request—Operations Support System (18)	Information
OSS (19)	Interface Is Active and Operational—Operations Support System (19)	Information
OSS (20)	Interface Is Not Started or Is Not Operational—Operations Support System (20)	Minor
OSS (21)	Resource Reset—Operations Support System (21)	Information

Table 8-24 Cisco BTS 10200 Operations Support System Events (continued)

Event Type	Event Name	Event Severity
OSS (22)	One Peer In The Realm Is Out of Contact—Operations Support System (22)	Major
OSS (23)	All Peers in the Realm Are Out of Contact—Operations Support System (23)	Critical
OSS (24)	User Log In Sessions Have Reached the User Session Limit—Operations Support System (24)	Warning
OSS (25)	Event Keep Alive Checked—Operations Support System (25)	Information

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 no definition of a data column 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 8-20.

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 through 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 8-21.

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 8-21.

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 during the access of 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 8-21.

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 8-21.

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.

No Reply Received From Destination—Operations Support System (8)

The No Reply Received From Destination alarm (minor) indicates that no reply was 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 8-21.

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 8-22.

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.

User Session Count Is Approaching Threshold Limit—Operations Support System (12)

The User Session Count Is Approaching Threshold Limit event serves as a warning that the user session count is approaching the threshold limit. The primary cause of the warning event is that the user session count usage has reached the allowed limit. To correct the primary cause of the warning event, use the **report client_session** command to view all log in sessions. Use the **stop client_session** command to remove stale sessions.

User Session Count Exceeds Major Threshold Limit—Operations Support System (14)

The User Session Count Exceeds Major Threshold Limit alarm (major) indicates that the user session count has exceeded the major threshold limit. To troubleshoot and correct the cause of the User Session Count Exceeds Major Threshold Limit alarm, refer to the "User Session Count Exceeds Major Threshold Limit—Operations Support System (14)" section on page 8-22.

Session Has Been Removed by Session Control Policy—Operations Support System (16)

The Session Has Been Removed by Session Control Policy event serves as an information alert that the session has been removed by the session control policy. The event is informational and no further action is necessary.

Session Has Been Removed—Operations Support System (17)

The Session Has Been Removed event serves as an information alert that the session has been removed. The primary cause of the informational alert is that the session was removed because it was idle over the timeout limit.

Invalid Session Request—Operations Support System (18)

The Invalid Session Request event serves as an information alert that the noun, verb, or parameters of the **request** command are not valid. To correct the primary cause of the Invalid Session Request event, check and correct the **request** command.

Interface Is Active and Operational—Operations Support System (19)

The Interface Is Active and Operational event serves as an informational alert that the application interface is active and operational. The event is informational only and no further action is required.

Interface Is Not Started or Is Not Operational—Operations Support System (20)

The Interface Is Not Started or Is Not Operational alarm (minor) indicates that an application interface has failed to start or is not operational. To troubleshoot and correct the cause of the Interface Is Not Started or Is Not Operational alarm, refer to the "Interface Is Not Started or Is Not Operational—Operations Support System (20)" section on page 8-22.

Resource Reset—Operations Support System (21)

The Resource Reset event serves as an informational alert that the resource has been reset. The event is informational only and no further action is required.

One Peer In The Realm Is Out of Contact—Operations Support System (22)

The One Peer In The Realm Is Out of Contact alarm (major) indicates that the communication between the Cisco BTS 10200 EMS system and the HSS has experienced a problem or the HSS is experiencing a problem. To troubleshoot and correct the cause of the One Peer in the Realm is Out of Contact alarm, refer to the "One Peer in the Realm Is Out of Contact—Operations Support System (22)" section on page 8-22.

All Peers in the Realm Are Out of Contact—Operations Support System (23)

The All Peers in the Realm Are Out of Contact alarm (critical) indicates that the communication between the Cisco BTS 10200 EMS system and the HSS has experienced a problem, or the HSS is experiencing a problem, or the network interface of the Cisco BTS 10200 is experiencing a problem. To troubleshoot and correct the cause of the All Peers in the Realm are Out of Contact alarm, refer to the "All Peers in the Realm Are Out of Contact—Operations Support System (23)" section on page 8-22.

User Log In Sessions Have Reached the User Session Limit—Operations Support System (24)

The User Log In Sessions Have Reached the User Session Limit event serves as a warning that the user log in has been denied because the maximum session limit has been reached. To correct the cause of the warning, use the **show user_session_limit** command to view the user session limit and use the **change user_session_limit** command to change the user session limit.

Event Keep Alive Checked—Operations Support System (25)

The Event Keep Alive Checked event serves as an informational alert. There is not an issue if an event is sent out and received. No action is required if event is received. If an event is *not* received periodically, then there is an issue with events and alarms or the SNMP system. If events or alarms are not received, capture the SNMP, EVT, EVT2, and OMS logs and restart the SNMP Agent.

Troubleshooting Operations Support System Alarms

This section provides the information you need for monitoring and correcting operations support system alarms. Table 8-25 lists all of the operations support system alarms in numerical order and provides cross-references to each subsection.

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

Table 8-25 Cisco BTS 10200 Operations Support System 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 (10)	Queue Processing Module Database Management Index Failed With Error—Operations Support System (10)	Major
OSS (14)	User Session Count Exceeds Major Threshold Limit—Operations Support System (14)	Major
OSS (20)	Interface Is Not Started or Is Not Operational—Operations Support System (20)	Minor
OSS (22)	One Peer in the Realm Is Out of Contact—Operations Support System (22)	Major
OSS (23)	All Peers in the Realm Are Out of Contact—Operations Support System (23)	Critical

Undefined Variable in Known Set—Operations Support System (2)

The Undefined Variable in Known Set alarm (major) indicates that no definition of a data column 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.

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 through 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.

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.

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 during access of 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 a schema error. To correct the primary cause of the alarm, contact Cisco TAC for support.

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.

No Reply Received From Destination—Operations Support System (8)

The No Reply Received From Destination alarm (minor) indicates that no reply was 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 (that is, when there are no device failures) and the traffic is at or below the engineered level, then Cisco TAC technical support should be asked to investigate the cause. If components of the system are in the process of failing or being restored 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.

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 an **SQL** command. To correct the secondary cause of the alarm, contact Cisco TAC.

User Session Count Exceeds Major Threshold Limit—Operations Support System (14)

The User Session Count Exceeds Major Threshold Limit alarm (major) indicates that the user session count has exceeded the major threshold limit. The primary cause of the alarm is that the user session usage has reached maximum allowed limit. To troubleshoot and correct the primary cause of the alarm, use the **report client_session** command to view all log in sessions. Use the **stop client_session** command to remove stale sessions.

Interface Is Not Started or Is Not Operational—Operations Support System (20)

The Interface Is Not Started or Is Not Operational alarm (minor) indicates that application interface has failed to start or is not operational. To troubleshoot and correct the cause of the alarm, restart the application interface.

One Peer in the Realm Is Out of Contact—Operations Support System (22)

The One Peer in the Realm Is Out of Contact alarm (major) indicates that the communication between the Cisco BTS 10200 EMS system and the HSS has experienced a problem or the HSS is experiencing a problem. To troubleshoot and correct the cause of the alarm, investigate the network and the HSS.

All Peers in the Realm Are Out of Contact—Operations Support System (23)

The All Peers in the Realm Are Out of Contact alarm (critical) indicates that the communication between the Cisco BTS 10200 EMS system and the HSS has experienced a problem, or the HSS is experiencing a problem, or the network interface of the Cisco BTS 10200 is experiencing a problem. To troubleshoot and correct the cause of the alarm, investigate the network, the HSS, and the network interface of the EMS.

CHAPTER 9

Security Troubleshooting

Revised: August 10, 2011, OL-25016-01

Introduction

This chapter provides the information needed for monitoring and troubleshooting 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 for monitoring and correcting the security events
- Troubleshooting Security Alarms—Provides the information needed for troubleshooting and correcting the security alarms

Security Events and Alarms

This section provides a brief overview of the security events and alarms for the Cisco BTS 10200 Softswitch; the event and alarms are arranged in numerical order. Table 9-1 lists all of the security events and alarms by severity.

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

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	Information	Not Used
	Security (3)		Security (2)	Security (1)	
			Security (4)		
			Security (5)		
			Security (6)		
			Security (7)		

Security (1)

Table 9-2 lists the details of the Security (1) informational event. For additional information, refer to the "Test Report—Security (1)" section on page 9-7.

Table 9-2 Security (1) Details

Description	Test Report
Severity	Information
Threshold	100
Throttle	0

Security (2)

Table 9-3 lists the details of the Security (2) warning event. 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 9-7.

Table 9-3 Security (2) Details

Description	Invalid Credentials Presented by a Session Initiation Protocol Phone (Invalid Credentials Presented by a SIP Phone)
Severity	Warning
Threshold	100
Throttle	0
Datawords	Authentication User Name—STRING [33] From AOR—STRING [65] SIP Request Type—STRING [15] Sender IP—STRING [20]
Primary Cause	There are invalid credentials in Session Initiation Protocol (SIP) request.
Primary Action	Ensure that the password on the SIP phone matches the value provisioned in the Cisco BTS 10200.

Security (3)

Table 9-4 lists the details of the Security (3) major alarm. To troubleshoot and correct the cause of the alarm, refer to the "Internet Protocol Security Connection Down—Security (3)" section on page 9-9.

Table 9-4 Security (3) Details

Description	Internet Protocol Security Connection Down (IPSEC Connection Down)
Severity	Major
Threshold	100
Throttle	0
Primary Cause	The kerberized management server (KMS) fails to establish the pf_key socket with the Internet Protocol security (IPSEC) engine. This implies that the IPSEC engine is not running and that it may not be installed.
Primary Action	1. Verify that the IPSEC is installed and running in the kernel. 2. Reboot. 3. If problem persists, contact Cisco TAC.

Security (4)

Table 9-5 lists the details of the Security (4) warning event. 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 9-8.

Table 9-5 Security (4) Details

Description	Internet Protocol Security Media Terminal Adapter Key Establish Error (IPSEC MTA Key Establish Error)
Severity	Warning
Threshold	100
Throttle	0
Primary Cause	A failure to establish the IPSEC keys to a given media terminal adapter (MTA) through the use of the kerberized key management protocol has occurred.
Primary Action	Validate the kerberos and the MTA device provisioning.

Security (5)

Table 9-6 lists the details of the Security (5) warning event. 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 9-8.

Table 9-6 Security (5) Details

Description	Internet Protocol Security Outgoing Security Association Not Found (IPSEC Outgoing SA Not Found)
Severity	Warning
Threshold	100
Throttle	0
Primary Cause	The KMS receives SA-missing messages 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. This action is based on the assumption that security is provisioned.

Security (6)

Table 9-7 lists the details of the Security (6) warning event. To monitor and correct the cause of the event, refer to the "Secure Session Initiation Protocol Endpoint Validation Failure—Security (6)" section on page 9-8.

Table 9-7 Security (6) Details

Description	Secure Session Initiation Protocol Endpoint Validation Failure (Secure SIP 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	There is erroneous provisioning in the Cisco BTS 10200.
Primary Action	Check if correct value of Secure-FQDN is provisioned in the Cisco BTS 10200.
Secondary Cause	There is erroneous provisioning in the domain name system (DNS).
Secondary Action	Verify the resolution of the Secure-FQDN in the DNS.
Ternary Cause	There is erroneous provisioning in the customer premises equipment (CPE).
Ternary Action	Verify the CPE provisioning to ensure that the correct source Internet Protocol (IP)/contact is used.

Security (7)

Table 9-8 lists the details of the Security (7) warning event. To monitor and correct the cause of the event, refer to the "Authentication Based On Credentials Failed—Security (7)" section on page 9-8.

Table 9-8 Security (7) Details

Description	Authentication Based On Credentials Failed
Severity	WARNING
Threshold	100
Throttle	0
Datawords	Auth User - STRING [32] Auth Realm - STRING [64] TGN-ID - FOUR_BYTES SIP Request Message - STRING [32]
Primary Cause	The trunk group provided invalid credentials.
Primary Action	Correct the provisioning of the username and password at the trunk group.

Monitoring Security Events

This section provides the information you need for monitoring and correcting security events. Table 9-9 lists all of the security events in numerical order and provides cross-references to each subsection.

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

Table 9-9 Cisco BTS 10200 Security Events

Event Type	Event Name	Event Severity
Security (1)	Test Report—Security (1)	Information
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
Security (7)	Authentication Based On Credentials Failed—Security (7)	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.

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 9-9.

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 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 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.

Authentication Based On Credentials Failed—Security (7)

The Authentication Based On Credentials Failed event serves as a warning that an authentication based on username and password credentials had failed. The primary cause of the event is that the associated trunk group provided invalid credentials. To correct the primary cause of the event, correct the provisioning of the username and password credentials at the trunk group.

Troubleshooting Security Alarms

This section provides the information you need for monitoring and correcting security alarms. Table 9-10 lists all of the security alarms in numerical order and provides cross-references to each subsection.

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

Table 9-10 Cisco BTS 10200 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 correct the 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.

CHAPTER 10

Signaling Troubleshooting

Revised: August 10, 2011, OL-25016-01

Introduction

This chapter provides the information needed for monitoring and troubleshooting 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 for monitoring and correcting the Signaling events
- Troubleshooting Signaling Alarms—Provides the information needed for troubleshooting and correcting the 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; the event and alarms are arranged in numerical order. Table 10-1 lists all of the signaling events and alarms by severity.

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

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	Information	Not Used
Signaling (12)	Signaling (7)	Signaling (10)	Signaling (4)	Signaling (1)	Signaling (2)
Signaling (64)	Signaling (8)	Signaling (14)	Signaling (6)	Signaling (42)	Signaling (3)
Signaling (65)	Signaling (9)	Signaling (15)	Signaling (25)	Signaling (43)	Signaling (5)
Signaling (69)	Signaling (11)	Signaling (16)	Signaling (26)	Signaling (44)	Signaling (35)
Signaling (75)	Signaling (13)	Signaling (17)	Signaling (27)	Signaling (45)	Signaling (37)
Signaling (80)	Signaling (19)	Signaling (18)	Signaling (28)	Signaling (46)	Signaling (38)
Signaling (81)	Signaling (20)	Signaling (22)	Signaling (29)	Signaling (49)	Signaling (39)
Signaling (82)	Signaling (21)	Signaling (24)	Signaling (30)	Signaling (50)	Signaling (41)
Signaling (83)	Signaling (23)	Signaling (36)	Signaling (31)	Signaling (51)	Signaling (47)
Signaling (84)	Signaling (40)	Signaling (78)	Signaling (32)	Signaling (52)	Signaling (48)
Signaling (85)	Signaling (59)	Signaling (92)	Signaling (33)	Signaling (53)	Signaling (56)
Signaling (107)	Signaling (63)	Signaling (93)	Signaling (34)	Signaling (54)	Signaling (67)
Signaling (110)	Signaling (66)	Signaling (94)	Signaling (60)	Signaling (55)	Signaling (123)
Signaling (119)	Signaling (68)	Signaling (95)	Signaling (70)	Signaling (57)	Signaling (128)
Signaling (120)	Signaling (79)	Signaling (96)	Signaling (71)	Signaling (58)	Signaling (129)
Signaling (142)	Signaling (86)	Signaling (97)	Signaling (72)	Signaling (61)	Signaling (130)
Signaling (144)	Signaling (87)	Signaling (98)	Signaling (73)	Signaling (62)	Signaling (131)
Signaling (153)	Signaling (88)	Signaling (99)	Signaling (74)	Signaling (76)	Signaling (148)
Signaling (154)	Signaling (89)	Signaling (100)	Signaling (115)	Signaling (77)	Signaling (149)
Signaling (162)	Signaling (90)	Signaling (101)	Signaling (132)	Signaling (104)	
Signaling (173)	Signaling (91)	Signaling (102)	Signaling (138)	Signaling (105)	
Signaling (174)	Signaling (103)	Signaling (106)	Signaling (141)	Signaling (133)	
Signaling (175)	Signaling (108)	Signaling (112)	Signaling (146)	Signaling (134)	
Signaling (176)	Signaling (109)	Signaling (117)	Signaling (147)	Signaling (135)	
	Signaling (111)	Signaling (118)	Signaling (158)	Signaling (136)	

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

Critical	Major	Minor	Warning	Information	Not Used
	Signaling (113)	Signaling (124)	Signaling (159)	Signaling (137)	
	Signaling (114)	Signaling (143)	Signaling (160)	Signaling (139)	
	Signaling (116)	Signaling (145)	Signaling (161)	Signaling (140)	
	Signaling (121)	Signaling (150)	Signaling (165)	Signaling (152)	
	Signaling (122)	Signaling (151)	Signaling (166)	Signaling (155)	
	Signaling (125)	Signaling (170)	Signaling (167)	Signaling (169)	
	Signaling (126)	Signaling (171)	Signaling (168)	Signaling (178)	
	Signaling (127)		Signaling (177)		
	Signaling (156)				
	Signaling (157)				
	Signaling (163)				
	Signaling (164)				
	Signaling (172)				
	Signaling (179)				
	Signaling (182)				

Signaling (1)

Table 10-2 lists the details of the Signaling (1) informational event. For additional information, refer to the "Test Report—Signaling (1)" section on page 10-103.

Table 10-2 Signaling (1) Details

Description	Test Report
Severity	Information
Threshold	10000
Throttle	0

Signaling (2)

Signaling (2) is not used.

Signaling (3)

Signaling (3) is not used.

Signaling (4)

Table 10-3 lists the details of the Signaling (4) warning event. To monitor and correct the cause of the event, refer to the "Invalid Message Received—Signaling (4)" section on page 10-103.

Table 10-3 Signaling (4) Details

Description	Invalid Message Received
Severity	Warning
Threshold	100
Throttle	0
Datawords	Endpoint Name—STRING [40] Message Type—STRING [40]
Primary Cause	This event is 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 reprovisioned.

Signaling (5)

Signaling (5) is not used.

Signaling (6)

Table 10-4 lists the details of the Signaling (6) warning event. To monitor and correct the cause of the event, refer to the "Database Module Function Call Failure—Signaling (6)" section on page 10-103.

Table 10-4 Signaling (6) Details

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 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)

Table 10-5 lists the details of the Signaling (7) major alarm. To troubleshoot and correct the cause of the alarm, refer to the "Socket Failure—Signaling (7)" section on page 10-136.

Table 10-5 Signaling (7) Details

Description	Socket Failure
Severity	Major
Threshold	30
Throttle	0
Datawords	Reason Text—STRING [30]
Primary Cause	Issued when there is a failure in creating or binding to the User Datagram Protocol (UDP) socket.
Primary Action	Verify that there is no conflict in the port assignment with other processes in the system and ensure that no previous instance of the same process is still running.
Secondary Cause	A software logic problem has occurred.
Secondary Action	Contact the Cisco Technical Assistance Center (TAC).

Signaling (8)

Table 10-6 lists the details of the Signaling (8) major alarm. To troubleshoot and correct the cause of the alarm, refer to the "Session Initiation Protocol Message Receive Failure—Signaling (8)" section on page 10-137.

Table 10-6 Signaling (8) Details

Description	Session Initiation Protocol Message Receive Failure (SIP Message Receive Failure)
Severity	Major
Threshold	30
Throttle	0
Datawords	Reason Text—STRING [50]
Primary Cause	Operating system level network errors have occurred or an invalid network configuration exists.
Primary Action	Have your network administrator resolve the network errors. Contact Cisco TAC if you need assistance. Manually clear the alarm. Restart this call agent instance using the **platform start** command.

Signaling (9)

Table 10-7 lists the details of the Signaling (9) major alarm. To troubleshoot and correct the cause of the alarm, refer to the "Timeout on Internet Protocol Address—Signaling (9)" section on page 10-137.

Table 10-7 Signaling (9) Details

Description	Timeout on Internet Protocol Address (Timeout on IP 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 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 the **control mgw** command to put it in service.

Signaling (10)

Table 10-8 lists the details of the Signaling (10) minor alarm. 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 10-138.

Table 10-8 Signaling (10) Details

Description	Failed to Send Complete Session Initiation Protocol Message (Failed to Send Complete SIP Message)
Severity	Minor
Threshold	100
Throttle	0
Datawords	Destination Address—STRING [64]
Primary Cause	Notifies the user that the Session Initiation Protocol (SIP) stack failed to send a SIP message because the message exceeded 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.

Signaling (11)

Table 10-9 lists the details of the Signaling (11) major alarm. 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 10-138.

Table 10-9 Signaling (11) Details

Description	Failed to Allocate Session Initiation Protocol Control Block (Failed to Allocate SIP Control Block)
Severity	Major
Threshold	100
Throttle	0
Datawords	Size—TWO_BYTES 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 for the changes to take effect.

Signaling (12)

Table 10-10 lists the details of the Signaling (12) critical alarm. 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 10-138.

Table 10-10 Signaling (12) Details

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	The feature server platform is down or is not operating properly.
Primary Action	Restart the applicable feature server.

Signaling (13)

Table 10-11 lists the details of the Signaling (13) major alarm. To troubleshoot and correct the cause of the alarm, refer to the "Signaling System 7 Signaling Link Down—Signaling (13)" section on page 10-138.

Table 10-11 Signaling (13) Details

Description	Signaling System 7 Signaling Link Down (SS7 Signaling Link Down)
Severity	Major
Threshold	100
Throttle	0
Datawords	Link_Number—ONE_BYTE Link_Name—STRING [25]
Primary Cause	The Signaling System 7 (SS7) trunk group may be out-of-service (OOS).
Primary Action	Use the **control ss7-trunk-grp** command 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	The SS7 link may be disconnected or faulty.
Ternary Action	Check the Ulticom local configuration.
Subsequent Cause	The remote SS7 signaling site may be down or incorrectly configured.
Subsequent Action	Check the Ulticom remote configuration.

Signaling (14)

Table 10-12 lists the details of the Signaling (14) minor alarm. To troubleshoot and correct the cause of the alarm, refer to the "Link Is Remotely Inhibited—Signaling (14)" section on page 10-139.

Table 10-12 Signaling (14) Details

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 the events at the network level for any that are related to the specified SS7 link. Restorative actions need to be taken on the remote end.

Signaling (15)

Table 10-13 lists the details of the Signaling (15) minor alarm. To troubleshoot and correct the cause of the alarm, refer to the "Link Is Locally Inhibited—Signaling (15)" section on page 10-139.

Table 10-13 Signaling (15) Details

Description	Link is Locally Inhibited
Severity	Minor
Threshold	100
Throttle	0
Datawords	Link Number—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 nonoperational, restore it to service.

Signaling (16)

Table 10-14 lists the details of the Signaling (16) minor alarm. To troubleshoot and correct the cause of the alarm, refer to the "Link Is Congested—Signaling (16)" section on page 10-139.

Table 10-14 Signaling (16) Details

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)

Table 10-15 lists the details of the Signaling (17) minor alarm. To troubleshoot and correct the cause of the alarm, refer to the "Link: Local Processor Outage—Signaling (17)" section on page 10-139.

Table 10-15 Signaling (17) Details

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 the underlying platform instances that support the specified SS7 link. Verify that the process and or platform are restarted and returned to service.

Signaling (18)

Table 10-16 lists the details of the Signaling (18) minor alarm. To troubleshoot and correct the cause of the alarm, refer to the "Link: Remote Processor Outage—Signaling (18)" section on page 10-139.

Table 10-16 Signaling (18) Details

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)

Table 10-17 lists the details of the Signaling (19) major alarm. To troubleshoot and correct the cause of the alarm, refer to the "Link Set Inaccessible—Signaling (19)" section on page 10-139.

Table 10-17 Signaling (19) Details

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)

Table 10-18 lists the details of the Signaling (20) major alarm. To troubleshoot and correct the cause of the alarm, refer to the "Link Set Congestion—Signaling (20)" section on page 10-140.

Table 10-18 Signaling (20) Details

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)

Table 10-19 lists the details of the Signaling (21) major alarm. To troubleshoot and correct the cause of the alarm, refer to the "Route Set Failure—Signaling (21)" section on page 10-140.

Table 10-19 Signaling (21) Details

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 to verify its restoral to service.

Signaling (22)

Table 10-20 lists the details of the Signaling (22) minor alarm. To troubleshoot and correct the cause of the alarm, refer to the "Route Set Congested—Signaling (22)" section on page 10-140.

Table 10-20 Signaling (22) Details

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 the 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)

Table 10-21 lists the details of the Signaling (23) major alarm. To troubleshoot and correct the cause of the alarm, refer to the "Destination Point Code Unavailable—Signaling (23)" section on page 10-141.

Table 10-21 Signaling (23) Details

Description	Destination Point Code Unavailable (DPC Unavailable)
Severity	Major
Threshold	200
Throttle	0
Datawords	DPC—STRING [12]
Primary Cause	Issued when the specified destination point code (DPC) is not available. This is usually caused by one of the following: 1. A failure in the affected DPC. 2. An unavailable route between the Cisco BTS 10200 and the affected DPC.
Primary Action	Verify that an alternate routing has been assigned for traffic destined to the affected DPC.

Signaling (24)

Table 10-22 lists the details of the Signaling (24) minor alarm. To troubleshoot and correct the cause of the alarm, refer to the "Destination Point Code Congested—Signaling (24)" section on page 10-142.

Table 10-22 Signaling (24) Details

Description	Destination Point Code Congested (DPC 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 the 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)

Table 10-23 lists the details of the Signaling (25) warning event. To monitor and correct the cause of the event, refer to the "Unanswered Blocking Message—Signaling (25)" section on page 10-106.

Table 10-23 Signaling (25) Details

Description	Unanswered Blocking Message (Unanswered BLO)
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 are 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)

Table 10-24 lists the details of the Signaling (26) warning event. To monitor and correct the cause of the event, refer to the "Unanswered Unblocking Message—Signaling (26)" section on page 10-106.

Table 10-24 Signaling (26) Details

Description	Unanswered Unblocking Message (Unanswered UBL)
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 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 are 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)

Table 10-25 lists the details of the Signaling (27) warning event. To monitor and correct the cause of the event, refer to the "Unanswered Circuit Group Blocking Message—Signaling (27)" section on page 10-107.

Table 10-25 Signaling (27) Details

Description	Unanswered Circuit Group Blocking Message (Unanswered CGB)
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 are 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)

Table 10-26 lists the details of the Signaling (28) warning event. To monitor and correct the cause of the event, refer to the "Unanswered Circuit Group Unblocking Message—Signaling (28)" section on page 10-107.

Table 10-26 Signaling (28) Details

Description	Unanswered Circuit Group Unblocking Message (Unanswered CGU)
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 are 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)

Table 10-27 lists the details of the Signaling (29) warning event. To monitor and correct the cause of the event, refer to the "Unanswered Circuit Query Message—Signaling (29)" section on page 10-107.

Table 10-27 Signaling (29) Details

Description	Unanswered Circuit Query Message (Unanswered CQM)
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 are 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)

Table 10-28 lists the details of the Signaling (30) warning event. To monitor and correct the cause of the event, refer to the "Unanswered Circuit Validation Test Message—Signaling (30)" section on page 10-108.

Table 10-28 Signaling (30) Details

Description	Unanswered Circuit Validation Test Message (Unanswered CVT)
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 are 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)

Table 10-29 lists the details of the Signaling (31) warning event. To monitor and correct the cause of the event, refer to the "Unanswered Reset Circuit Message—Signaling (31)" section on page 10-108.

Table 10-29 Signaling (31) Details

Description	Unanswered Reset Circuit Message (Unanswered RSC)
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 are 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)

Table 10-30 lists the details of the Signaling (32) warning event. To monitor and correct the cause of the event, refer to the "Unanswered Group Reset Message—Signaling (32)" section on page 10-108.

Table 10-30 Signaling (32) Details

Description	Unanswered Group Reset Message (Unanswered GRS)
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 are 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)

Table 10-31 lists the details of the Signaling (33) warning event. To monitor and correct the cause of the event, refer to the "Unanswered Release Message—Signaling (33)" section on page 10-109.

Table 10-31 Signaling (33) Details

Description	Unanswered Release Message (Unanswered REL)
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 are 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)

Table 10-32 lists the details of the Signaling (34) warning event. To monitor and correct the cause of the event, refer to the "Unanswered Continuity Check Request Message—Signaling (34)" section on page 10-109.

Table 10-32 Signaling (34) Details

Description	Unanswered Continuity Check Request Message (Unanswered CCR)
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 are 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 (35)

Signaling (35) is not used.

Signaling (36)

Table 10-33 lists the details of the Signaling (36) minor alarm. To troubleshoot and correct the cause of the alarm, refer to the "Trunk Locally Blocked—Signaling (36)" section on page 10-142.

Table 10-33 Signaling (36) Details

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	No action required.

Signaling (37)

Signaling (37) is not used.

Signaling (38)

Signaling (38) is not used.

Signaling (39)

Signaling (39) is not used.

Signaling (40)

Table 10-34 lists the details of the Signaling (40) major alarm. To troubleshoot and correct the cause of the alarm, refer to the "Trunk Remotely Blocked—Signaling (40)" section on page 10-142.

Table 10-34 Signaling (40) Details

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 an SS7 trunk. Issued when a service OOS message is received for Integrated Services Digital Network (ISDN) trunks. Issued when Reverse Make Busy (RBZ) signal is received for channel-associated signaling (CAS) operator trunk.
Primary Action	No action required. You can manually recover from this condition locally by controlling the affected trunks to the unequipped (UEQP) state and back to the INS state.

Signaling (41)

Signaling (41) is not used.

Signaling (42)

Table 10-35 lists the details of the Signaling (42) informational event. For additional information, refer to the "Continuity Testing Message Received on the Specified Circuit Identification Code—Signaling (42)" section on page 10-110.

Table 10-35 Signaling (42) Details

Description	Continuity Testing Message Received on the Specified Circuit Identification Code (COT Message Received on the Specified CIC)
Severity	Information
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)

Table 10-36 lists the details of the Signaling (43) informational event. 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 10-110.

Table 10-36 Signaling (43) Details

Description	Release Complete Received in Response to Reset Circuit Message on the Specified Circuit Identification Code (RLC Received in Response to RSC Message on the Specified CIC)
Severity	Information
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 an RSC message on the specified CIC.
Primary Action	No action required.

Signaling (44)

Table 10-37 lists the details of the Signaling (44) informational event. For additional information, refer to the "Continuity Recheck Is Performed on Specified Circuit Identification Code—Signaling (44)" section on page 10-110.

Table 10-37 Signaling (44) Details

Description	Continuity Recheck is Performed on Specified Circuit Identification Code (Continuity Recheck is Performed on Specified CIC)
Severity	Information
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)

Table 10-38 lists the details of the Signaling (45) informational event. For additional information, refer to the "Circuit Is Unequipped on Remote Side—Signaling (45)" section on page 10-110.

Table 10-38 Signaling (45) Details

Description	Circuit is Unequipped on Remote Side
Severity	Information
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 find out if an existing circuit was unequipped causing a status mismatch with the local end.

Signaling (46)

Table 10-39 lists the details of the Signaling (46) informational event. For additional information, refer to the "Specified Circuit Identification Code Is Invalid for the Operation—Signaling (46)" section on page 10-110.

Table 10-39 Signaling (46) Details

Description	Specified Circuit Identification Code is Invalid for the Operation (Specified CIC is Invalid for the Operation)
Severity	Information
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.

Signaling (47)

Signaling (47) is not used.

Signaling (48)

Signaling (48) is not used.

Signaling (49)

Table 10-40 lists the details of the Signaling (49) informational event. For additional information, refer to the "A General Processing Error Encountered—Signaling (49)" section on page 10-111.

Table 10-40 Signaling (49) Details

Description	A General Processing Error Encountered
Severity	Information
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 ensure proper operation.

Signaling (50)

Table 10-41 lists the details of the Signaling (50) informational event. For additional information, refer to the "Unexpected Message for the Call State Is Received: Clear Call—Signaling (50)" section on page 10-111.

Table 10-41 Signaling (50) Details

Description	Unexpected Message for the Call State is Received: Clear Call
Severity	Information
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 ensure proper operation.

Signaling (51)

Table 10-42 lists the details of the Signaling (51) informational event. For additional information, refer to the "Set Trunk State as Remotely Unequipped—Signaling (51)" section on page 10-111.

Table 10-42 Signaling (51) Details

Description	Set Trunk State as Remotely Unequipped
Severity	Information
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 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)

Table 10-43 lists the details of the Signaling (52) informational event. For additional information, refer to the "Set Trunk State as Not Remotely Blocked—Signaling (52)" section on page 10-111.

Table 10-43 Signaling (52) Details

Description	Set Trunk State as Not Remotely Blocked
Severity	Information
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)

Table 10-44 lists the details of the Signaling (53) informational event. For additional information, refer to the "Set Trunk State as Remotely Blocked—Signaling (53)" section on page 10-111.

Table 10-44 Signaling (53) Details

Description	Set Trunk State as Remotely Blocked
Severity	Information
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)

Table 10-45 lists the details of the Signaling (54) informational event. For additional information, refer to the "Circuit Validation Test Aborted—Signaling (54)" section on page 10-111.

Table 10-45 Signaling (54) Details

Description	Circuit Validation Test Aborted
Severity	Information
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 failed a validation test due to an internal failure.
Primary Action	Verify that the SS7 signaling adapter process and the SS7 interface are operating normally.

Signaling (55)

Table 10-46 lists the details of the Signaling (55) informational event. For additional information, refer to the "Circuit Validation Successful—Signaling (55)" section on page 10-112.

Table 10-46 Signaling (55) Details

Description	Circuit Validation Successful
Severity	Information
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.

Signaling (56)

Signaling (56) is not used.

Signaling (57)

Table 10-47 lists the details of the Signaling (57) informational event. For additional information, refer to the "Continuity Recheck Failed—Signaling (57)" section on page 10-112.

Table 10-47 Signaling (57) Details

Description	Continuity Recheck Failed
Severity	Information
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 that the SS7 signaling adapter process and the SS7 interface are operating normally.

Signaling (58)

Table 10-48 lists the details of the Signaling (58) informational event. For additional information, refer to the "Continuity Recheck Successful—Signaling (58)" section on page 10-112.

Table 10-48 Signaling (58) Details

Description	Continuity Recheck Successful
Severity	Information
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)

Table 10-49 lists the details of the Signaling (59) major alarm. 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 10-142.

Table 10-49 Signaling (59) Details

Description	Auto State Change for Integrated Services Digital Network Trunk Group by Media Gateway (Auto State Change for ISDN Trunk Group by Media Gateway)
Severity	Major
Threshold	100
Throttle	0
Datawords	Trunk Group ID—FOUR_BYTES 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)

Table 10-50 lists the details of the Signaling (60) warning event. 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 10-112.

Table 10-50 Signaling (60) Details

Description	Integrated Services Digital Network Status Message Containing Error Indication Received (ISDN Status Message Containing Error Indication Received)
Severity	Warning
Threshold	100
Throttle	0
Datawords	Termination Name—STRING [40] 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 the service state.

Signaling (61)

Table 10-51 lists the details of the Signaling (61) informational event. For additional information, refer to the "Trunk Operational State Changed by Service Message—Signaling (61)" section on page 10-112.

Table 10-51 Signaling (61) Details

Description	Trunk Operational State Changed by Service Message
Severity	Information
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 by 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)

Table 10-52 lists the details of the Signaling (62) informational event. For additional information, refer to the "Received Integrated Services Digital Network Restart Message—Signaling (62)" section on page 10-113.

Table 10-52 Signaling (62) Details

Description	Received Integrated Services Digital Network Restart Message (Received ISDN Restart Message)
Severity	Information
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)

Table 10-53 lists the details of the Signaling (63) major alarm. To troubleshoot and correct the cause of the alarm, refer to the "Media Gateway/Termination Faulty—Signaling (63)" section on page 10-142.

Table 10-53 Signaling (63) Details

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, an unknown package type, an 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)

Table 10-54 lists the details of the Signaling (64) critical alarm. 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 10-143.

Table 10-54 Signaling (64) Details

Description	Media Gateway Adapter Running out of Shared Memory Pools (MGA Running out of Shared Memory Pools)
Severity	Critical
Threshold	100
Throttle	0
Primary Cause	Issued when the Media Gateway Control Protocol (MGCP) signaling adapter was unable to allocate data storage for an inter-process communication (IPC) message due to a lack of resources.
Primary Action	Contact Cisco TAC for assistance.

Signaling (65)

Table 10-55 lists the details of the Signaling (65) critical alarm. 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 10-143.

Table 10-55 Signaling (65) Details

Description	Media Gateway Adapter Running out of Heap Memory (MGA Running out of Heap Memory)
Severity	Critical
Threshold	100
Throttle	0
Primary Cause	Issued when the MGCP signaling adapter was unable to allocate data storage for an IPC message from the heap due to a lack of resources.
Primary Action	Contact Cisco TAC for assistance.

Signaling (66)

Table 10-56 lists the details of the Signaling (66) major alarm. 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 10-143.

Table 10-56 Signaling (66) Details

Description	Call Agent Internal Error (Because of Which Media Gateway Adapter has to Start Automatically) (CA Internal Error (Because of Which MGA has to Start Automatically))
Severity	Major
Threshold	100
Throttle	0
Datawords	Fully Qualified Name—STRING [80] 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 the log files to Cisco TAC for analysis and corrective action.

Signaling (67)

Signaling (67) is not used.

Signaling (68)

Signaling (68) is not used.

Signaling (69)

Table 10-57 lists the details of the Signaling (69) critical alarm. To troubleshoot and correct the cause of the alarm, refer to the "Call Agent Is Not Up or Is Not Responding to the Feature Server—Signaling (69)" section on page 10-143.

Table 10-57 Signaling (69) Details

Description	Call Agent is not Up or is not Responding to the Feature Server
Severity	Critical
Threshold	100
Throttle	0
Datawords	Configured CA Name—STRING [70]
Primary Cause	The Call Agent (CA) to Feature Server (FS) link has had a communication failure due to wrong system configuration; or the CA or FS is down.
Primary Action	Check the configuration related to the CA to FS communication link. Check the FS table entries and the CA entry.

Signaling (70)

Table 10-58 lists the details of the Signaling (70) warning event. 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 10-114.

Table 10-58 Signaling (70) Details

Description	Integrated Services Digital Network Unable to Restore D-channel Due to Failed Communication (ISDN Unable to Restore D-channel Due to Failed Communication)
Severity	Warning
Threshold	100
Throttle	0
Datawords	Trunk Group ID—FOUR_BYTES 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 that the provisioning of the backhaul port is correct at both the call agent and media gateway.

Signaling (71)

Table 10-59 lists the details of the Signaling (71) warning event. 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 10-114.

Table 10-59 Signaling (71) Details

Description	Integrated Services Digital Network Unable to Establish D-channel (ISDN Unable to Establish D-channel)
Severity	Warning
Threshold	100
Throttle	0
Datawords	Trunk Group ID—FOUR_BYTES 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)

Table 10-60 lists the details of the Signaling (72) warning event. 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 10-114.

Table 10-60 Signaling (72) Details

Description	Integrated Services Digital Network—Calls Lost Due to D-channel Down for Period of Time (ISDN—Calls Lost Due to D-channel Down for Period of Time)
Severity	Warning
Threshold	100
Throttle	0
Datawords	Trunk Group ID—FOUR_BYTES 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 the connection between the private branch exchange (PBX) and the media gateway.
Primary Action	Resupply power to the media gateway and verify that the connection between the PBX and the media gateway is intact.

Signaling (73)

Table 10-61 lists the details of the Signaling (73) warning event. 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 10-114.

Table 10-61 Signaling (73) Details

Description	Integrated Services Digital Network—Unable to Send Restart Due to Restart Timer Expired (ISDN—Unable to Send Restart Due to Restart Timer Expired)
Severity	Warning
Threshold	100
Throttle	0
Datawords	Termination Name—STRING [40] 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)

Table 10-62 lists the details of the Signaling (74) warning event. 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 10-115.

Table 10-62 Signaling (74) Details

Description	Integrated Services Digital Network: Unable to Send the Service Due to the Service Timer Expired (ISDN: Unable to Send the Service Due to the Service Timer Expired)
Severity	Warning
Threshold	100
Throttle	0
Datawords	Termination Name—STRING [40] 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 service timer is set to an appropriate level.

Signaling (75)

Table 10-63 lists the details of the Signaling (75) critical alarm. To troubleshoot and correct the cause of the alarm, refer to the "Signaling System 7 Stack Not Ready—Signaling (75)" section on page 10-143.

Table 10-63 Signaling (75) Details

Description	Signaling System 7 Stack Not Ready (SS7 Stack Not Ready)
Severity	Critical
Threshold	100
Throttle	0
Datawords	LogicalName—STRING [64]
Primary Cause	SS7 stack is not configured properly.
Primary Action	Check SS7 stack configuration.
Secondary Cause	SS7 stack is not up and functioning.
Secondary Action	Check SS7 stack status. Execute the platform **start -i omni** command to bring up SS7 stack.

Signaling (76)

Table 10-64 lists the details of the Signaling (76) informational event. For additional information, refer to the "Timeout on Remote Instance—Signaling (76)" section on page 10-115.

Table 10-64 Signaling (76) Details

Description	Timeout on Remote Instance
Severity	Information
Threshold	100
Throttle	0
Datawords	Port Number—TWO_BYTES Hostname—STRING [64]
Primary Cause	The communication between the call agent and the remote instance is faulty.
Primary Action	No action needed.

Signaling (77)

Table 10-65 lists the details of the Signaling (77) informational event. For additional information, refer to the "Integrated Services Digital Network D-Channel Switchover for Not Facility Associated Signaling—Signaling (77)" section on page 10-115.

Table 10-65 Signaling (77) Details

Description	Integrated Services Digital Network D-channel Switchover for Not Facility Associated Signaling (ISDN D-channel Switchover for NFAS)
Severity	Information
Threshold	100
Throttle	0
Datawords	Trunk Group ID—FOUR_BYTES Trunk Group Index—FOUR_BYTES
Primary Cause	The D-channels were manually switched through use of the command line interface (CLI).
Primary Action	Verify the operator action.
Secondary Cause	The active D-channel is lost.
Secondary Action	Verify that the gateway is operational and that the connection to the PBX is good.

Signaling (78)

Table 10-66 lists the details of the Signaling (78) minor alarm. To troubleshoot and correct the cause of the alarm, refer to the "Integrated Services Digital Network Single D-Channel Down for Not Facility Associated Signaling—Signaling (78)" section on page 10-144.

Table 10-66 Signaling (78) Details

Description	Integrated Services Digital Network Single D-channel Down for Not Facility Associated Signaling (ISDN Single D-channel Down for NFAS)
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 the primary rate interface (PRI) is down.
Primary Action	Check the gateway power and the gateway connection to the PBX.

Signaling (79)

Table 10-67 lists the details of the Signaling (79) major alarm. To troubleshoot and correct the cause of the alarm, refer to the "Trunking Gateway Unreachable—Signaling (79)" section on page 10-144.

Table 10-67 Signaling (79) Details

Description	Trunking 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	The Trunking Gateway is not responding to keep-alive Audit Endpoint messages.
Primary Action	Check the IP connectivity status between Cisco BTS 10200 Call Agent and the Trunking Gateway.

Signaling (80)

Table 10-68 lists the details of the Signaling (80) critical alarm. To troubleshoot and correct the cause of the alarm, refer to the "Out of Bounds, Memory/Socket Error—Signaling (80)" section on page 10-144.

Table 10-68 Signaling (80) Details

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	Increase the random access memory (RAM) and contact Cisco TAC.
Secondary Cause	Out of IPC pool memory.
Secondary Action	Resize the IPC pool size in the platform configuration file.
Ternary Cause	A socket error has occurred. An inappropriate or already bound socket is in use.
Ternary Action	Check the UDP port supplied with the media gateway adapter (MGA) command-line for validity and prior use.

Signaling (81)

Table 10-69 lists the details of the Signaling (81) critical alarm. To troubleshoot and correct the cause of the alarm, refer to the "Insufficient Heap Memory—Signaling (81)" section on page 10-144.

Table 10-69 Signaling (81) Details

Description	Insufficient Heap Memory
Severity	Critical
Threshold	100
Throttle	0
Datawords	Gateway ID—STRING [32]
Primary Cause	Issued when the H.323 Protocol (H.323) signaling adapter is unable to allocate memory from the system.
Primary Action	Contact Cisco TAC for assistance.

Signaling (82)

Table 10-70 lists the details of the Signaling (82) critical alarm. To troubleshoot and correct the cause of the alarm, refer to the "Insufficient Shared Memory Pools—Signaling (82)" section on page 10-144.

Table 10-70 Signaling (82) Details

Description	Insufficient Shared Memory Pools
Severity	Critical
Threshold	100
Throttle	0
Datawords	Gateway ID—STRING [32]
Primary Cause	Issued when the H.323 signaling adapter was unable to allocate storage.
Primary Action	Contact Cisco TAC for corrective action.

Signaling (83)

Table 10-71 lists the details of the Signaling (83) critical alarm. To troubleshoot and correct the cause of the alarm, refer to the "Error While Binding to Socket—Signaling (83)" section on page 10-145.

Table 10-71 Signaling (83) Details

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]
Primary Cause	An error has occurred while the system was binding to a socket.
Primary Action	Contact Cisco TAC.

Signaling (84)

Table 10-72 lists the details of the Signaling (84) critical alarm. To troubleshoot and correct the cause of the alarm, refer to the "Reached Maximum Socket Limit—Signaling (84)" section on page 10-145.

Table 10-72 Signaling (84) Details

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 the platform.cfg file is wrong.
Primary Action	Reconfigure the platform.cfg file and restart the H3A process.

Signaling (85)

Table 10-73 lists the details of the Signaling (85) critical alarm. To troubleshoot and correct the cause of the alarm, refer to the "Initialization Failure—Signaling (85)" section on page 10-145.

Table 10-73 Signaling (85) Details

Description	Initialization Failure
Severity	Critical
Threshold	100
Throttle	0
Datawords	Gateway ID—STRING [32] Reason—STRING [128]
Primary Cause	A process initialization failure has occurred.
Primary Action	Check Dataword 2 (Reason) for the failure cause and take action accordingly.

Signaling (86)

Table 10-74 lists the details of the Signaling (86) major alarm. To troubleshoot and correct the cause of the alarm, refer to the "Remote H.323 Gateway Is Not Reachable—Signaling (86)" section on page 10-145.

Table 10-74 Signaling (86) Details

Description	Remote H.323 Gateway is not Reachable
Severity	Major
Threshold	100
Throttle	0
Datawords	Gateway ID—STRING [32] Remote GW TSAP Addr—STRING [32]
Primary Cause	A loss of communication with a remote gateway has occurred.
Primary Action	Perform the standard connectivity tests—both the physical checks and the IP tests. Also, ensure that the gateway is not out of service.

Signaling (87)

Table 10-75 lists the details of the Signaling (87) major alarm. To troubleshoot and correct the cause of the alarm, refer to the "H.323 Message Parsing Error—Signaling (87)" section on page 10-145.

Table 10-75 Signaling (87) Details

Description	H.323 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 H.323 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 its content or contact Cisco TAC.

Signaling (88)

Table 10-76 lists the details of the Signaling (88) major alarm. To troubleshoot and correct the cause of the alarm, refer to the "H.323 Message Encoding Error—Signaling (88)" section on page 10-145.

Table 10-76 Signaling (88) Details

Description	H.323 Message Encoding Error
Severity	Major
Threshold	100
Throttle	0
Datawords	Gateway ID—STRING [32] Reason—STRING [128]
Primary Cause	Unable to encode an H.323 message for sending.
Primary Action	This is indicative of a software bug. Contact Cisco TAC.

Signaling (89)

Table 10-77 lists the details of the Signaling (89) major alarm. To troubleshoot and correct the cause of the alarm, refer to the "Gatekeeper not Available/Reachable—Signaling (89)" section on page 10-146.

Table 10-77 Signaling (89) Details

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	The gatekeeper is not available or is unreachable.
Primary Action	Check network connectivity. Check to ensure that the gatekeeper (GK) is reachable by trying to ping GK IP address. If the GK is reachable, check to ensure that the GK is configured up.

Signaling (90)

Table 10-78 lists the details of the Signaling (90) major alarm. To troubleshoot and correct the cause of the alarm, refer to the "Alternate Gatekeeper Is Not Responding—Signaling (90)" section on page 10-146.

Table 10-78 Signaling (90) Details

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	The alternate gatekeeper is not responding.
Primary Action	Check network connectivity. Check to ensure that the alternate GK is reachable by trying to ping the alternate GK IP address. If the GK is reachable, check to ensure that the alternate GK is configured up.

Signaling (91)

Table 10-79 lists the details of the Signaling (91) major alarm. To troubleshoot and correct the cause of the alarm, refer to the "Endpoint Security Violation—Signaling (91)" section on page 10-146.

Table 10-79 Signaling (91) Details

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 H.323 security violation has occurred.
Primary Action	The password on the Cisco BTS 10200 and/or the gatekeeper is wrong—the H.323 gateway (H.323GW) table may not be provisioned properly or there is a time synchronization problem between the Cisco BTS 10200 and/or gatekeeper and the Network Time Protocol (NTP) server. Ensure that both the Cisco BTS 10200 and the gatekeeper are pointing to the same NTP server.

Signaling (92)

Table 10-80 lists the details of the Signaling (92) minor alarm. To troubleshoot and correct the cause of the alarm, refer to the "Invalid Call Identifier—Signaling (92)" section on page 10-146.

Table 10-80 Signaling (92) Details

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	There is a software problem on the Cisco BTS 10200 or on an endpoint. Contact Cisco TAC.

Signaling (93)

Table 10-81 lists the details of the Signaling (93) minor alarm. To troubleshoot and correct the cause of the alarm, refer to the "Invalid Call Reference Value—Signaling (93)" section on page 10-146.

Table 10-81 Signaling (93) Details

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	There is a software problem on the Cisco BTS 10200 or on an endpoint. Contact Cisco TAC.

Signaling (94)

Table 10-82 lists the details of the Signaling (94) minor alarm. To troubleshoot and correct the cause of the alarm, refer to the "Invalid Conference Identifier—Signaling (94)" section on page 10-146.

Table 10-82 Signaling (94) Details

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	There is a software problem on the Cisco BTS 10200 or on an endpoint. Contact Cisco TAC.

Signaling (95)

Table 10-83 lists the details of the Signaling (95) minor alarm. To troubleshoot and correct the cause of the alarm, refer to the "Invalid Message from the Network—Signaling (95)" section on page 10-147.

Table 10-83 Signaling (95) Details

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	An unsupported or invalid message type received from network.
Primary Action	Contact Cisco TAC.

Signaling (96)

Table 10-84 lists the details of the Signaling (96) minor alarm. To troubleshoot and correct the cause of the alarm, refer to the "Internal Call Processing Error—Signaling (96)" section on page 10-147.

Table 10-84 Signaling (96) Details

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	Contact Cisco TAC.

Signaling (97)

Table 10-85 lists the details of the Signaling (97) minor alarm. To troubleshoot and correct the cause of the alarm, refer to the "Insufficient Information to Complete Call—Signaling (97)" section on page 10-147.

Table 10-85 Signaling (97) Details

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	Contact Cisco TAC.

Signaling (98)

Table 10-86 lists the details of the Signaling (98) minor alarm. To troubleshoot and correct the cause of the alarm, refer to the "H.323 Protocol Inconsistencies—Signaling (98)" section on page 10-147.

Table 10-86 Signaling (98) Details

Description	H.323 Protocol Inconsistencies
Severity	Minor
Threshold	100
Throttle	0
Datawords	Gateway ID—STRING [32] Call ID—EIGHT_BYTES Reason—STRING [128]
Primary Cause	The H.323 endpoint and the Cisco BTS 10200 are running different protocol versions.
Primary Action	This is only an issue where the endpoint is running a higher version of the H.323 protocol than the Cisco BTS 10200. Contact Cisco TAC.

Signaling (99)

Table 10-87 lists the details of the Signaling (99) minor alarm. To troubleshoot and correct the cause of the alarm, refer to the "Abnormal Call Clearing—Signaling (99)" section on page 10-147.

Table 10-87 Signaling (99) Details

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	Contact Cisco TAC.

Signaling (100)

Table 10-88 lists the details of the Signaling (100) minor alarm. To troubleshoot and correct the cause of the alarm, refer to the "Codec Negotiation Failed—Signaling (100)" section on page 10-147.

Table 10-88 Signaling (100) Details

Description	Codec Negotiation Failed
Severity	Minor
Threshold	100
Throttle	0
Datawords	Gateway ID—STRING [32] Call ID—EIGHT_BYTES Reason—STRING [128]
Primary Cause	The codec negotiation has failed.
Primary Action	Find a compatible set of codec settings for both sides, reprovision the endpoints of the call, and try the call again.

Signaling (101)

Table 10-89 lists the details of the Signaling (101) minor alarm. To troubleshoot and correct the cause of the alarm, refer to the "Per Call Security Violation—Signaling (101)" section on page 10-147.

Table 10-89 Signaling (101) Details

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)

Table 10-90 lists the details of the Signaling (102) minor alarm. To troubleshoot and correct the cause of the alarm, refer to the "H.323 Network Congested—Signaling (102)" section on page 10-148.

Table 10-90 Signaling (102) Details

Description	H.323 Network Congested
Severity	Minor
Threshold	100
Throttle	0
Datawords	Gateway ID—STRING [32] Gatekeeper ID—STRING [32]
Primary Cause	The H.323 application process has depleted its 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.

Signaling (103)

Table 10-91 lists the details of the Signaling (103) major alarm. To troubleshoot and correct the cause of the alarm, refer to the "Aggregation Connection Down—Signaling (103)" section on page 10-148.

Table 10-91 Signaling (103) Details

Description	Aggregation Connection Down (AGGR Connection Down)
Severity	Major
Threshold	100
Throttle	0
Datawords	AGGR-ID—STRING [16]
Primary Cause	The Transmission Control Protocol (TCP) connection is down.
Primary Action	Check the associated cabling and perform a ping to test the connectivity.

Signaling (104)

Table 10-92 lists the details of the Signaling (104) informational event. For additional information, refer to the "Aggregation Unable to Establish Connection—Signaling (104)" section on page 10-119.

Table 10-92 Signaling (104) Details

Description	Aggregation Unable To Establish Connection (AGGR Unable To Establish Connection)
Severity	Information
Threshold	100
Throttle	0
Datawords	AGGR-ID—STRING [16]
Primary Cause	A TCP connection establish failure has occurred.
Primary Action	Check the IP connectivity of the call agent (CA) and the cable modem termination system (CMTS).

Signaling (105)

Table 10-93 lists the details of the Signaling (105) informational event. For additional information, refer to the "Aggregation Gate Set Failed—Signaling (105)" section on page 10-119.

Table 10-93 Signaling (105) Details

Description	Aggregation Gate Set Failed (AGGR Gate Set Failed)
Severity	Information
Threshold	100
Throttle	0
Datawords	AGGR-ID—STRING [16] Error-Code—TWO_BYTES Sub-Error-Code—TWO_BYTES
Primary Cause	The gate set acknowledgement never came from the CMTS.
Primary Action	None

Signaling (106)

Table 10-94 lists the details of the Signaling (106) minor alarm. To troubleshoot and correct the cause of the alarm, refer to the "Enhanced Subscriber Authentication Cisco BTS 10200 Delivery Function Connection Down—Signaling (106)" section on page 10-148.

Table 10-94 Signaling (106) Details

Description	Enhanced Subscriber Authentication Cisco BTS 10200 Delivery Function Connection Down (ESA Cisco BTS 10200 DF Connection Down)
Severity	Minor
Threshold	100
Throttle	0
Primary Cause	The delivery function (DF) server is not responding.
Primary Action	Check the encryption key or the IP connectivity to the DF server.

Signaling (107)

Table 10-95 lists the details of the Signaling (107) critical alarm. To troubleshoot and correct the cause of the alarm, refer to the "Logical Internet Protocol Addresses Not Mapped Correctly—Signaling (107)" section on page 10-148.

Table 10-95 Signaling (107) Details

Description	Logical Internet Protocol Addresses not Mapped Correctly (Logical IP Addresses not Mapped Correctly)
Severity	Critical
Threshold	30
Throttle	0
Datawords	Contact Domain Name—STRING [128] Number of IP Addresses Resolved—FOUR_BYTES Number of Virtual IP Addresses—FOUR_BYTES
Primary Cause	A contact name in the configuration file is not configured in the domain name system (DNS).
Primary Action	Verify that the name in the DNS matches the name in the platform.cfg and opticall.cfg files.
Secondary Cause	A contact could not be resolved to an IP address on the host.
Secondary Action	Verify that the DNS resolves to the IP addresses reserved for the process on the Cisco BTS 10200.
Ternary Cause	The IP address manager is not running.
Ternary Action	Verify that the Internet Protocol Manager (IPM) process is running and check for alarms from the IPM.
Subsequent Cause	A mis-configuration occurred during installation or manual changes were made after installation.
Subsequent Action	Contact Cisco TAC for support.

Signaling (108)

Table 10-96 lists the details of the Signaling (108) major alarm. To troubleshoot and correct the cause of the alarm, refer to the "Simplex Only Operational Mode—Signaling (108)" section on page 10-148.

Table 10-96 Signaling (108) Details

Description	Simplex Only Operational Mode
Severity	Major
Threshold	30
Throttle	0
Datawords	Host Domain Name—STRING [128]
Primary Cause	The hostname parameter is specified in the platform.cfg file instead of being specified in the -contact parameter.
Primary Action	Check to see if the Cisco BTS 10200 is configured as a simplex system.

Signaling (109)

Table 10-97 lists the details of the Signaling (109) major alarm. To troubleshoot and correct the cause of the alarm, refer to the "Stream Control Transmission Protocol Association Failure—Signaling (109)" section on page 10-149.

Table 10-97 Signaling (109) Details

Description	Stream Control Transmission Protocol Association Failure (SCTP Association Failure)
Severity	Major
Threshold	100
Throttle	0
Datawords	SCTP Association ID—STRING [17]
Primary Cause	The Ethernet cables for the signaling gateway process (SGP) are unplugged or severed.
Primary Action	Plug Ethernet cables in or fix the severed connection.
Secondary Cause	SGP is not operational.
Secondary Action	Check the SGP alarms to determine why SGP is not operating properly.

Signaling (110)

Table 10-98 lists the details of the Signaling (110) critical alarm. To troubleshoot and correct the cause of the alarm, refer to the "Signaling Gateway Group Is Out of Service—Signaling (110)" section on page 10-152.

Table 10-98 Signaling (110) Details

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 the CA and the SGs are out-of-service.
Primary Action	Make sure all Ethernet connections on the CA and the SGs are plugged in. Also make sure all of the associated IP routers are operational.
Secondary Cause	The MTP3 user adapter (M3UA) layer is down between the CA and the SGs.
Secondary Action	Use the Cisco snooper application to determine why the M3UA layer is down.

Signaling (111)

Table 10-99 lists the details of the Signaling (111) major alarm. 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 10-153.

Table 10-99 Signaling (111) Details

Description	Stream Control Transmission Protocol Association Degraded (One of Two Internet Protocol Connections Down) (SCTP Association Degraded (One of Two IP connections Down))
Severity	Major
Threshold	100
Throttle	0
Datawords	SCTP Association ID—STRING [17] Destination IP Address—STRING [11]
Primary Cause	A single Ethernet connection on the CA or the SGP is unplugged or severed.
Primary Action	Plug in all of the Ethernet connections or repair if severed.
Secondary Cause	An SCTP communication problem—protocol timeout.
Secondary Action	Use the Cisco snooper application to determine why the SCTP association is degraded.

Signaling (112)

Table 10-100 lists the details of the Signaling (112) minor alarm. To troubleshoot and correct the cause of the alarm, refer to the "Stream Control Transmission Protocol Association Configuration Error—Signaling (112)" section on page 10-154.

Table 10-100 Signaling (112) Details

Description	Stream Control Transmission Protocol Association Configuration Error (SCTP Association Configuration Error)
Severity	Minor
Threshold	100
Throttle	0
Datawords	SCTP Association ID—STRING [17]
Primary Cause	The destination IP address is invalid.
Primary Action	Input a new destination IP address—see log for additional details.
Secondary Cause	The local IP address is invalid.
Secondary Action	Input new local IP address information.
Ternary Cause	The IP Routing table is not configured properly.
Ternary Action	Have the system administrator configure the IP Routing table.

Signaling (113)

Table 10-101 lists the details of the Signaling (113) major alarm. To troubleshoot and correct the cause of the alarm, refer to the "Signaling Gateway Failure—Signaling (113)" section on page 10-155.

Table 10-101 Signaling (113) Details

Description	Signaling Gateway Failure
Severity	Major
Threshold	100
Throttle	0
Datawords	Signaling Gateway ID—STRING [17]
Primary Cause	All of the associated signaling gateway processes are out-of-service.
Primary Action	Determine why each of the associated SGP processes is out-of-service (see the SGP alarm definition).

Signaling (114)

Table 10-102 lists the details of the Signaling (114) major alarm. To troubleshoot and correct the cause of the alarm, refer to the "Signaling Gateway Process Is Out of Service—Signaling (114)" section on page 10-155.

Table 10-102 Signaling (114) Details

Description	Signaling Gateway Process is Out-of-Service
Severity	Major
Threshold	100
Throttle	0
Datawords	Signaling Gateway—STRING [17]
Primary Cause	All of the SCTP associations between the SGP and the CA are out-of-service.
Primary Action	See the SCTP association alarm definition to determine how to rectify the problem.
Secondary Cause	The M3UA layer is down between the CA and the SGP.
Secondary Action	Use the Cisco snooper utility to determine why M3UA layer is down. Also see the log for additional information.

Signaling (115)

Table 10-103 lists the details of the Signaling (115) warning event. To monitor and correct the cause of the event, refer to the "Invalid Routing Context Received—Signaling (115)" section on page 10-121.

Table 10-103 Signaling (115) Details

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	The routing context was configured improperly on the CA or the signaling gateway (SG).
Primary Action	Reconfigure the routing context on the CA or the SG so that it matches in both places.

Signaling (116)

Table 10-104 lists the details of the Signaling (116) major alarm. To troubleshoot and correct the cause of the alarm, refer to the "Destination Point Code User Part Unavailable—Signaling (116)" section on page 10-156.

Table 10-104 Signaling (116) Details

Description	Destination Point Code User Part Unavailable (DPC User Part Unavailable)
Severity	Major
Threshold	100
Throttle	0
Datawords	DPC ID—STRING [17]
Primary Cause	An SGP sent a destination user part unavailable (DUPU) M3UA message to the CA indicating that a User Part is unavailable on a DPC.
Primary Action	Contact the SS7 Network Administrator to report the User Part Unavailable problem on the DPC so that communication can be restored.

Signaling (117)

Table 10-105 lists the details of the Signaling (117) minor alarm. 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 10-156.

Table 10-105 Signaling (117) Details

Description	Circuit Validation Test Message Received for an Unequipped Circuit Identification Code (CVT Message Received for an Unequipped CIC)
Severity	Minor
Threshold	100
Throttle	0
Datawords	CIC—TWO_BYTES TGN-ID—EIGHT_BYTES DPC—STRING [13]
Primary Cause	The CIC is not provisioned
Primary Action	Provision the CIC.

Signaling (118)

Table 10-106 lists the details of the Signaling (118) minor alarm. To troubleshoot and correct the cause of the alarm, refer to the "Circuit Verification Response Received With Failed Indication—Signaling (118)" section on page 10-156.

Table 10-106 Signaling (118) Details

Description	Circuit Verification Response Received with Failed Indication (CVR 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	A CIC mismatch occurred.
Primary Action	Perform an internal test such as checking that the CIC is assigned to a circuit between the sending and the receiving switch.

Signaling (119)

Table 10-107 lists the details of the Signaling (119) critical alarm. To troubleshoot and correct the cause of the alarm, refer to the "Signaling System 7 Adapter Process Faulty—Signaling (119)" section on page 10-156.

Table 10-107 Signaling (119) Details

Description	Signaling System 7 Adapter Process Faulty (S7A Process Faulty)
Severity	Critical
Threshold	100
Throttle	0
Datawords	Reason—STRING [36]
Primary Cause	An OMNI or S7A exception has occurred.
Primary Action	Check the OMNI process. The S7A will restart itself if the S7A maximum number of restarts is not exceeded.

Signaling (120)

Table 10-108 lists the details of the Signaling (120) critical alarm. 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 10-156.

Table 10-108 Signaling (120) Details

Description	Signaling System 7 Module/Signaling System 7 Adapter Faulty (S7M/S7A Faulty)
Severity	Critical
Threshold	100
Throttle	0
Datawords	Reason—STRING [36]
Primary Cause	An OMNI failure has occurred.
Primary Action	Check the OMNI status; a failover will occur in a duplex configuration.

Signaling (121)

Table 10-109 lists the details of the Signaling (121) major alarm. 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 10-157.

Table 10-109 Signaling (121) Details

Description	Message Transfer Part 3 User Adapter Cannot Go Standby (M3UA/SUA Cannot Go Standby)
Severity	Major
Threshold	100
Throttle	0
Datawords	Platform ID—STRING [17]
Primary Cause	No inactive acknowledge (ACK) messages are received from any SG or SCTP. The associations are probably down.
Primary Action	Investigate any other alarms to see if SGs are down or the SCTP associations are down. Take corrective action according to those alarms.

Signaling (122)

Table 10-110 lists the details of the Signaling (122) major alarm. 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 10-157.

Table 10-110 Signaling (122) Details

Description	Message Transfer Part 3 User Adapter Cannot Go Active (M3UA/SUA Cannot Go Active)
Severity	Major
Threshold	100
Throttle	0
Datawords	Platform ID—STRING [17]
Primary Cause	No active acknowledgement messages are being received from any SG or SCTP. The associations are probably down.
Primary Action	Investigate any other alarms to see if the SGs are down or the SCTP associations are down. Take corrective action according to those alarms.

Signaling (123)

Signaling (123) is not used.

Signaling (124)

Table 10-111 lists the details of the Signaling (124) minor alarm. To troubleshoot and correct the cause of the alarm, refer to the "Remote Subsystem is Out Of Service—Signaling (124)" section on page 10-157.

Table 10-111 Signaling (124) Details

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	A link loss has occurred or the remote subsystem is out of service.
Primary Action	Check the links. Check the remote location, if possible.

Signaling (125)

Table 10-112 lists the details of the Signaling (125) major alarm. To troubleshoot and correct the cause of the alarm, refer to the "Signaling Connection Control Part Routing Error—Signaling (125)" section on page 10-157.

Table 10-112 Signaling (125) Details

Description	Signaling Connection Control Part Routing Error (SCCP Routing Error)
Severity	Major
Threshold	100
Throttle	0
Primary Cause	The signaling connection control part (SCCP) route is invalid or is not available.
Primary Action	Provision the right SCCP route.

Signaling (126)

Table 10-113 lists the details of the Signaling (126) major alarm. To troubleshoot and correct the cause of the alarm, refer to the "Signaling Connection Control Part Binding Failure—Signaling (126)" section on page 10-158.

Table 10-113 Signaling (126) Details

Description	Signaling Connection Control Part Binding Failure (SCCP Binding Failure)
Severity	Major
Threshold	100
Throttle	0
Datawords	Local Point Code—STRING [20] Local Subsystem Numb—ONE_BYTE
Primary Cause	A Trillium stack binding failure has occurred.
Primary Action	Reinitialize the TCAP signaling adapter (TSA) process or remove the subsystem from the Element Management System (EMS) table and add it again.

Signaling (127)

Table 10-114 lists the details of the Signaling (127) major alarm. To troubleshoot and correct the cause of the alarm, refer to the "Transaction Capabilities Application Part Binding Failure—Signaling (127)" section on page 10-158.

Table 10-114 Signaling (127) Details

Description	Transaction Capabilities Application Part Binding Failure (TCAP Binding Failure)
Severity	Major
Threshold	100
Throttle	0
Primary Cause	A Trillium stack binding failure has occurred.
Primary Action	Reinitialize the TSA process or remove the subsystem from the EMS table and add it again.

Signaling (128)

Signaling (128) is not used.

Signaling (129)

Signaling (129) is not used.

Signaling (130)

Signaling (130) is not used.

Signaling (131)

Signaling (131) is not used.

Signaling (132)

Table 10-115 lists the details of the Signaling (132) warning event. 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 10-123.

Table 10-115 Signaling (132) Details

Description	Transaction Capabilities Application Part Reaches the Provisioned Resource Limit (TCAP Reaches the Provisioned Resource Limit)
Severity	Warning
Threshold	100
Throttle	0
Datawords	Dialogue/Invoke ID—FOUR_BYTES
Primary Cause	The Transaction Capabilities Application Part (TCAP) has run out of all the preconfigured dialogue IDs or invoke IDs.

Signaling (133)

Table 10-116 lists the details of the Signaling (133) informational event. For additional information, refer to the "Unable to Decode Generic Transport Descriptor Message—Signaling (133)" section on page 10-123.

Table 10-116 Signaling (133) Details

Description	Unable to Decode Generic Transport Descriptor Message (Unable to Decode GTD Message)
Severity	Information
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)

Table 10-117 lists the details of the Signaling (134) informational event. For additional information, refer to the "Signaling System 7 Message Encoding Failure—Signaling (134)" section on page 10-124.

Table 10-117 Signaling (134) Details

Description	Signaling System 7 Message Encoding Failure (SS7 Message Encoding Failure)
Severity	Information
Threshold	100
Throttle	0
Datawords	CIC Number—TWO_BYTES TGN-ID—FOUR_BYTES DPC—STRING [20] OPC—STRING [20]
Primary Cause	An error in the ISDN user part (ISUP) stack or in a signaling adapter interface (SAI) message has occurred.
Primary Action	Capture the SS7 trace of circuit for examination by support personnel and contact Cisco TAC.

Signaling (135)

Table 10-118 lists the details of the Signaling (135) informational event. For additional information, refer to the "Signaling System 7 Message Decoding Failure—Signaling (135)" section on page 10-124.

Table 10-118 Signaling (135) Details

Description	Signaling System 7 Message Decoding Failure (SS7 Message Decoding Failure)
Severity	Information
Threshold	100
Throttle	0
Datawords	CIC Number—TWO_BYTES TGN-ID—FOUR_BYTES DPC—STRING [20] OPC—STRING [20]
Primary Cause	An error in the ISUP stack or in an SAI message has occurred.
Primary Action	Capture the SS7 trace of circuit for examination by support personnel and contact Cisco TAC.

Signaling (136)

Table 10-119 lists the details of the Signaling (136) informational event. For additional information, refer to the "Signaling System 7 Message Invalid Received—Signaling (136)" section on page 10-124.

Table 10-119 Signaling (136) Details

Description	Signaling System 7 Message Invalid Received (SS7 Message Invalid Received)
Severity	Information
Threshold	100
Throttle	0
Datawords	CIC Number—TWO_BYTES TGN-ID—FOUR_BYTES DPC—STRING [20] OPC—STRING [20]
Primary Cause	An invalid message was received from the line in the ISUP stack.
Primary Action	Capture the SS7 trace of circuit for examination by support personnel and contact Cisco TAC.
Secondary Cause	An invalid message was received from the line in the ISUP stack.
Secondary Action	Verify that the signal switching point (SSP) sending the message to the CA is correctly configured.

Signaling (137)

Table 10-120 lists the details of the Signaling (137) informational event. For additional information, refer to the "Signaling System 7 Confusion Message Received—Signaling (137)" section on page 10-124.

Table 10-120 Signaling (137) Details

Description	Signaling System 7 Confusion Message Received (SS7 Confusion Message Received)
Severity	Information
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 a parameter received was not recognized or understood.
Primary Action	Check the log for more information (including confusion (CFN) diagnostic output). Capture an SS7 trace of the affected circuits. If the diagnostic data indicates that messages or parameters that must be supported are being dropped, refer the captured data to Cisco TAC along with a description of the call scenario.

Signaling (138)

Table 10-121 lists the details of the Signaling (138) warning event. 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 10-124.

Table 10-121 Signaling (138) Details

Description	Number of Open Session Initiation Protocol Connections is Reaching Engineered Limit (Number of Open SIP 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	A call failure has occurred or a feature is unavailable.
Primary Action	The system configuration and the 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 TAC.

Signaling (139)

Table 10-122 lists the details of the Signaling (139) informational event. For additional information, refer to the "Signaling System 7 Trunk was Found to be in Erroneous State—Signaling (139)" section on page 10-125.

Table 10-122 Signaling (139) Details

Description	Signaling System 7 Trunk was Found to be in Erroneous State (SS7 Trunk was Found to be in Erroneous State)
Severity	Information
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	A discrepancy between the local and the remote trunk states has occurred.
Primary Action	Automatic corrective action is enforced when using American National Standards Institute (ANSI) ISUP.

Signaling (140)

Table 10-123 lists the details of the Signaling (140) informational event. For additional information, refer to the "Unanswered Information Message—Signaling (140)" section on page 10-125.

Table 10-123 Signaling (140) Details

Description	Unanswered Information Message (Unanswered INF Message)
Severity	Information
Threshold	100
Throttle	0
Datawords	CIC—TWO_BYTES TGN-ID—FOUR_BYTES DPC—STRING [20] OPC—STRING [20]
Primary Cause	The far-end switch is not responding to an information (INF) message with an information request (INR) message.
Primary Action	Verify that the far-end switch can correctly respond to an INF message.

Signaling (141)

Table 10-124 lists the details of the Signaling (141) warning event. 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 10-125.

Table 10-124 Signaling (141) Details

Description	Address not Resolved by Domain Name System Server (Address not Resolved by DNS Server)
Severity	Warning
Threshold	100
Throttle	0
Datawords	TSAP_Address/Hostname—STRING [256] Reason—STRING [64]
Primary Cause	The transport service access point (TSAP) address or hostname is not defined in the DNS.
Primary Action	Add an entry for the TSAP address to the DNS server, or fix the Cisco BTS 10200 provisioning.

Signaling (142)

Table 10-125 lists the details of the Signaling (142) critical alarm. 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 10-158.

Table 10-125 Signaling (142) Details

Description	Session Initiation Protocol Trunk Operationally Out-of-Service (SIP Trunk Operationally out of Service)
Severity	Critical
Threshold	100
Throttle	0
Datawords	Trunk Group Description —STRING [21] Trunk SIP Element ID—STRING [65] Trunk Server Group ID—STRING [65]
Primary Cause	Issued when the Cisco BTS 10200 is unable to communicate with a remote SIP party (Call-Agent or Proxy) over a SIP or a SIP-T trunk.
Primary Action	Verify that the DNS resolution exists, if TSAP address of the remote entity is a domain name. Verify that 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, verify that the network connection is operational.
Secondary Cause	The 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 that the SIP application is running on the remote host and is listening on the port specified in the TSAP address.

Signaling (143)

Table 10-126 lists the details of the Signaling (143) minor alarm. 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 10-158.

Table 10-126 Signaling (143) Details

Description	Internet Protocol Interface Link to the Signaling System 7 Signaling Gateway is Down (IP Interface Link to the SS7 Signaling Gateway is Down)
Severity	Minor
Threshold	100
Throttle	0
Datawords	Interface Name—STRING [65] Interface IP Address—STRING [65]
Primary Cause	A hardware problem has occurred.
Primary Action	Check the link interfaces.

Signaling (144)

Table 10-127 lists the details of the Signaling (144) critical alarm. 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 10-158.

Table 10-127 Signaling (144) Details

Description	All Internet Protocol Interface Links to Signaling System 7 Signaling Gateway are Down (All IP Interface Links to SS7 Signaling Gateway are Down)
Severity	Critical
Threshold	100
Throttle	0
Datawords	Interface Name—STRING [65] Interface IP Address—STRING [65]
Primary Cause	A hardware problem has occurred.
Primary Action	Check the link interfaces.

Signaling (145)

Table 10-128 lists the details of the Signaling (145) minor alarm. 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 10-159.

Table 10-128 Signaling (145) Details

Description	One Internet Protocol Interface to Signaling System 7 Signaling Gateway is Down (One IP Interface to SS7 Signaling Gateway is Down)
Severity	Minor
Threshold	100
Throttle	0
Datawords	Interface Name—STRING [65] Interface IP Address—STRING [65]
Primary Cause	A hardware problem has occurred.
Primary Action	Check the link interfaces.

Signaling (146)

Table 10-129 lists the details of the Signaling (146) warning event. 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 10-126.

Table 10-129 Signaling (146) Details

Description	All Retransmission Attempts of Session Initiation Protocol Request or Response Failed (All Retransmission Attempts of SIP 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 the DNS or the IP address of request uniform resource identifier (URI). SIP response: All retransmission attempts for a SIP response failed for the received socket IP address of the request and the DNS (or the IP address) listed in the header.
Primary Action	Ensure that if the DNS server is up and running for the host name resolution and ensure that the DNS server is provisioned properly to resolve the correct order of the IP addresses. Ensure that the previous hop network component is alive and in a healthy state.

Signaling (147)

Table 10-130 lists the details of the Signaling (147) warning event. To monitor and correct the cause of the event, refer to the "Domain Name System Service Addresses Exhausted—Signaling (147)" section on page 10-126.

Table 10-130 Signaling (147) Details

Description	Domain Name System Service Addresses Exhausted (DNS SRV Addresses Exhausted)
Severity	Warning
Threshold	100
Throttle	0
Datawords	SRV Hostname—STRING [256]
Primary Cause	The DNS service (SRV) hostname resolution to the IP addresses is exhausted.
Primary Action	Add an entry to the SRV in the DNS server. Fix the Cisco BTS 10200 provisioning.

Signaling (148)

Signaling (148) is not used.

Signaling (149)

Signaling (149) is not used.

Signaling (150)

Table 10-131 lists the details of the Signaling (150) minor alarm. To troubleshoot and correct the cause of the alarm, refer to the "Stream Control Transmission Protocol Association Congested—Signaling (150)" section on page 10-159.

Table 10-131 Signaling (150) Details

Description	Stream Control Transmission Protocol Association Congested (SCTP Association Congested)
Severity	Minor
Threshold	100
Throttle	0
Datawords	SCTP Association ID—STRING [17] Congestion Level—ONE_BYTE
Primary Cause	The network is congested.
Primary Action	Clean off the network congestion caused by routing or switching issues.
Secondary Cause	The central processing unit (CPU) is throttled.
Secondary Action	You might need to upgrade to a more powerful platform or offload some traffic.

Signaling (151)

Table 10-132 lists the details of the Signaling (151) minor alarm. To troubleshoot and correct the cause of the alarm, refer to the "Subscriber Line Faulty—Signaling (151)" section on page 10-160.

Table 10-132 Signaling (151) Details

Description	Subscriber Line Faulty
Severity	Minor
Threshold	100
Throttle	0
Datawords	End Point /Termination - STRING [54] Media Gateway Type - STRING [54] Error Details - STRING [54]
Primary Cause	The residential gateway returned an error code in response to a command from the MGW.
Primary Action	Try controlling subscriber termination to OOS and back to INS using the Cisco BTS 10200 CLI command. If the problem persist after more calls, check the configuration in the Cisco BTS 10200 and the RGW. If the error codes returned by the MGW are harmless, the error codes can be suppressed by adding a new entry in the MGCP-RETCODE-ACTION table and by changing the EP-ACTION to reset/none.

Signaling (152)

Table 10-133 lists the details of the Signaling (151) informational event. For additional information, refer to the "Termination Transient Error Received—Signaling (152)" section on page 10-127.

Table 10-133 Signaling (152) Details

Description	Termination Transient Error Received
Severity	Information
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	Contact Cisco TAC.

Signaling (153)

Table 10-134 lists the details of the Signaling (153) critical alarm. To troubleshoot and correct the cause of the alarm, refer to the "Emergency Trunks Become Locally Blocked—Signaling (153)" section on page 10-160.

Table 10-134 Signaling (153) Details

Description	Emergency Trunks Become Locally Blocked
Severity	Critical
Threshold	100
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 an emergency trunk (CAS, SS7, or ISDN) gets locally blocked.
Primary Action	No action is required.

Signaling (154)

Table 10-135 lists the details of the Signaling (154) critical alarm. To troubleshoot and correct the cause of the alarm, refer to the "Emergency Trunks Become Remotely Blocked—Signaling (154)" section on page 10-160.

Table 10-135 Signaling (154) Details

Description	Emergency Trunks Become Remotely Blocked
Severity	Critical
Threshold	100
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 an emergency trunk (CAS, SS7, or ISDN) gets remotely blocked.
Primary Action	No action is required.

Signaling (155)

Table 10-136 lists the details of the Signaling (155) informational event. For additional information, refer to the "Packet Cable Multi-Media Unsolicited Gate Delete—Signaling (155)" section on page 10-127.

Table 10-136 Signaling (155) Details

Description	Packet Cable Multi-Media Unsolicited Gate Delete (PCMM Unsolicited Gate Delete)
Severity	Information
Threshold	100
Throttle	0
Datawords	AGGR-ID—STRING [16] Subscriber-IP-Address—STRING [32] Gate-Direction—STRING [16]
Primary Cause	An error condition has been encountered by the CMTS.
Primary Action	Check the alarms and warnings from the CMTS.

Signaling (156)

Table 10-137 lists the details of the Signaling (156) major alarm. To troubleshoot and correct the cause of the alarm, refer to the "Integrated Services Digital Network Signaling Gateway Down—Signaling (156)" section on page 10-161.

Table 10-137 Signaling (156) Details

Description	Integrated Services Digital Network Signaling Gateway Down (ISDN Signaling Gateway Down)
Severity	Major
Threshold	100
Throttle	0
Datawords	Media Gateway ID—STRING [16] Media Gateway TSAP Address—STRING [64]
Primary Cause	Cannot communicate to the ISDN gateway because it is down due to a failure in the gateway. The SCTP association might be down.
Primary Action	Check to see if the SCTP association is down due to an issue on the network.
Secondary Cause	The IUA layer might be down in the gateway.
Secondary Action	No action is needed. The IUA layer will be automatically recovered.

Signaling (157)

Table 10-138 lists the details of the Signaling (157) major alarm. To troubleshoot and correct the cause of the alarm, refer to the "Integrated Services Digital Network Signaling Gateway Inactive—Signaling (157)" section on page 10-161.

Table 10-138 Signaling (157) Details

Description	Integrated Services Digital Network Signaling Gateway Inactive (ISDN Signaling Gateway Inactive)
Severity	Major
Threshold	100
Throttle	0
Datawords	Media Gateway ID—STRING [16]
Primary Cause	A **shutdown** command was executed in the application server on the ISDN gateway side.
Primary Action	No action is needed. The ISDN gateway will be automatically recovered.

Signaling (158)

Table 10-139 lists the details of the Signaling (158) warning event. To monitor and correct the cause of the event, refer to the "Invalid Integrated Services Digital Network Interface Identification—Signaling (158)" section on page 10-128.

Table 10-139 Signaling (158) Details

Description	Invalid Integrated Services Digital Network Interface Identification (Invalid ISDN Interface ID)
Severity	Warning
Threshold	100
Throttle	0
Datawords	Received Interface ID—TWO_BYTES
Primary Cause	The interface ID is not configured correctly on the ISDN gateway side.
Primary Action	Configure the D-channel correctly on the gateway side. The D-channel configuration on the call-agent side should match with that on the gateway side.

Signaling (159)

Table 10-140 lists the details of the Signaling (159) warning event. To monitor and correct the cause of the event, refer to the "Integrated Services Digital Network User Adaptation Layer Cannot Go Active—Signaling (159)" section on page 10-128.

Table 10-140 Signaling (159) Details

Description	Integrated Services Digital Network User Adaptation Layer Cannot Go Active (IUA Cannot Go Active)
Severity	Warning
Threshold	100
Throttle	0
Datawords	Not applicable.
Primary Cause	No active acknowledgement messages are being received from any signaling gateway. The ISDN signaling gateway or the SCTP associations are probably down.
Primary Action	Investigate other alarms to see if the signaling gateways are down or the SCTP associations are down. Take corrective action according to those alarms.

Signaling (160)

Table 10-141 lists the details of the Signaling (160) warning event. To monitor and correct the cause of the event, refer to the "Integrated Services Digital Network User Adaptation Layer Cannot Go Standby—Signaling (160)" section on page 10-128.

Table 10-141 Signaling (160) Details

Description	Integrated Services Digital Network User Adaptation Layer Cannot Go Standby (IUA Cannot Go Standby)
Severity	Warning
Threshold	100
Throttle	0
Datawords	Not applicable.
Primary Cause	No UP acknowledgement messages are being received from any signaling gateway. The ISDN signaling gateway or the SCTP associations are probably down.
Primary Action	Investigate other alarms to see if the signaling gateways are down or the SCTP associations are down. Take corrective action according to those alarms.

Signaling (161)

Table 10-142 lists the details of the Signaling (161) warning event. To monitor and correct the cause of the event, refer to the "Session Initiation Protocol Update Not Allowed for Operator Service Position System Calls—Signaling (161)" section on page 10-128.

Table 10-142 Signaling (161) Details

Description	Session Initiation Protocol Update not Allowed for Operator Service Position System Calls (SIP Update not Allowed for OSPS Calls)
Severity	Warning
Threshold	100
Throttle	0
Datawords	Trunk Group Description—STRING [21] TSAP Address—STRING [65]
Primary Cause	The remote switch does not allow the Cisco BTS 10200 to send SIP UPDATE messages. The update message is mandatory in CMSS and is used exclusively by the Cisco BTS 10200 for operator service calls over SIP including BLV, emergency interrupt, and 911 ringback calls.
Primary Action	Upgrade or reprovision the remote switch so it can process incoming SIP update messages.

Signaling (162)

Table 10-143 lists the details of the Signaling (162) critical alarm. To troubleshoot and correct the cause of the alarm, refer to the "Session Initiation Protocol Server Group Element Operationally Out of Service—Signaling (162)" section on page 10-161.

Table 10-143 Signaling (162) Details

Description	Session Initiation Protocol Server Group Element Operationally Out of Service (SIP Server Group Element Operationally out of Service)
Severity	Critical
Threshold	100
Throttle	0
Datawords	Server Group Description—STRING [64] TSAP Address of the SIP-Element.—STRING [64]
Primary Cause	Issued when the Cisco BTS 10200 is unable to communicate with a remote SIP party (Call-Agent or Proxy) over a SIP server group element.
Primary Action	If the TSAP address of the remote entity is a domain name, verify that the DNS resolution exists. Verify that the remote entity is reachable by ICMP ping, using the TSAP address from the Event Report. If the same alarm is reported for other TSAP addresses on several softswitch trunk groups and/or server-group elements, verify that the network connection is operational.
Secondary Cause	The remote SIP party is not operational.
Secondary Action	If the ping is not successful, diagnose the issue that prevents the TSAP address from being reached. Verify that the SIP application is running on the remote host and listening on the port specified in the TSAP address.

Signaling (163)

Table 10-144 lists the details of the Signaling (163) major alarm. To troubleshoot and correct the cause of the alarm, refer to the "Routing Key Inactive—Signaling (163)" section on page 10-161.

Table 10-144 Signaling (163) Details

Description	Routing Key Inactive
Severity	Major
Threshold	100
Throttle	0
Datawords	Routing Key ID—STRING [17] Routing Context—STRING [17] Signaling Gateway ID—STRING [17]
Primary Cause	Inactive ACK messages were received from a Signaling Gateway. The SGs or the SCTP associations are probably down.
Primary Action	Investigate other alarms to see if the SGs are down or the SCTP associations are down. Take corrective action according to those alarms. Also check the AS status for the routing context on ITP.

Signaling (164)

Table 10-145 lists the details of the Signaling (164) major alarm. To troubleshoot and correct the cause of the alarm, refer to the "Signaling Gateway Traffic Mode Mismatch—Signaling (164)" section on page 10-162.

Table 10-145 Signaling (164) Details

Description	Signaling Gateway Traffic Mode Mismatch
Severity	Major
Threshold	100
Throttle	0
Datawords	Signaling Gateway ID—STRING [17] Signaling Gateway Process ID—STRING [17]
Primary Cause	The traffic mode does not match on the Cisco BTS 10200 and the Signaling Gateway.
Primary Action	Verify the AS traffic-mode configuration in the Signaling Gateway. Check that the SG internal redundancy mode for the traffic-mode setting has been set correctly in the Cisco BTS 10200.

Signaling (165)

Table 10-146 lists the details of the Signaling (165) warning event. To monitor and correct the cause of the event, refer to the "No Session Initiation Protocol P-DCS Billing Information Header Received—Signaling (165)" section on page 129.

Table 10-146 Signaling (165) Details

Description	No Session Initiation Protocol P-DCS Billing Information Header Received (No SIP P-DCS Billing Info Hdr Rcvd)
Severity	Warning
Threshold	10
Throttle	0
Datawords	Trunk Group ID—STRING [21] TSAP Address—STRING [65]
Primary Cause	The originating switch is not provisioned to add the P-DCS Billing Information header to outgoing SIP requests and responses.
Primary Action	Provision the originating switch to add the P-DCS Billing Information header to outgoing messages.
Secondary Cause	The header could have been stripped off by an intermediate proxy.
Secondary Action	Determine if the header has been stripped off by an intermediate proxy and, if it has, configure for corrective action if so.
Ternary Cause	There was a SIP message encode error at the sending switch.
Ternary Action	Determine if a SIP message encode error occurred at the sending switch and if so, call the technical assistance center to determine a fix for the problem.

Signaling (166)

Table 10-147 lists the details of the Signaling (166) warning event. To monitor and correct the cause of the event, refer to the "No Routing Keys Are Active—Signaling (166)" section on page 129.

Table 10-147 Signaling (166) Details

Description	No Routing Keys are Active
Severity	Warning
Threshold	0
Throttle	0
Primary Cause	Routing keys are not set to the active state.
Primary Action	Set the routing keys to the active state.
Secondary Cause	The ITP provisioning is incorrect.
Secondary Action	Check the ITP provisioning.

Signaling (167)

Table 10-148 lists the details of the Signaling (167) warning event. To monitor and correct the cause of the event, refer to the "No Signaling Gateways Are Active—Signaling (167)" section on page 130.

Table 10-148 Signaling (167) Details

Description	No Signaling Gateways are Active
Severity	Warning
Threshold	0
Throttle	0
Primary Cause	A communication problem between the ITP and the Cisco BTS 10200 has occurred.
Primary Action	Check the communication path between the Cisco BTS 10200 and the ITP.

Signaling (168)

Table 10-149 lists the details of the Signaling (168) warning event. To monitor and correct the cause of the event, refer to the "A Session Initiation Protocol Server Group Has No Child Elements Provisioned—Signaling (168)" section on page 130.

Table 10-149 Signaling (168) Details

Description	A Session Initiation Protocol Server Group has no Child Elements Provisioned (A SIP Server Group has no Child Elements Provisioned)
Severity	Warning
Threshold	100
Throttle	0
Datawords	Server Group ID—STRING [64]
Primary Cause	Issued when a SIP Server Group is provisioned as in-service but has no child elements provisioned.
Primary Action	This server group is considered administratively out of service. If that is acceptable, no action is required. If the group was expected to be workable, place the server group back out of service, resolve the provisioning problem, and place the group back in service.

Signaling (169)

Table 10-150 lists the details of the Signaling (169) informational event. For additional information, refer to the "Session Initiation Protocol Element Provisioned With Service Enabled Is Internally Disabled—Signaling (169)" section on page 130.

Table 10-150 Signaling (169) Details

Description	Session Initiation Protocol Element Provisioned with Service Enabled is Internally Disabled (SIP Element Provisioned with SRV Enabled is Internally Disabled)
Severity	Information
Threshold	100
Throttle	0
Datawords	SIP Element ID—STRING [64]
Primary Cause	A SIP element was provisioned with SRV enabled and is associated with at least one or more Server Groups.
Primary Action	The SRV flag will be assumed disabled. However, to resolve this informational message, provision the SRV flag disabled on the SIP element.

Signaling (170)

Table 10-151 lists the details of the Signaling (170) minor alarm. To troubleshoot and correct the cause of the alarm, refer to the "Residential Gateway Endpoints Are Out of Service at the Gateway—Signaling (170)" section on page 10-162.

Table 10-151 Signaling (170) Details

Description	Residential Gateway Endpoints are out of Service at the Gateway (Residential Gateway Endpoints are out of Service at the GW)
Severity	Minor
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	The residential gateway has been administratively taken OOS through use of the command at the GW.
Primary Action	Bring the residential gateway administratively into INS using the command at the GW.

Signaling (171)

Table 10-152 lists the details of the Signaling (171) minor alarm. To troubleshoot and correct the cause of the alarm, refer to the "Residential Gateway Unreachable—Signaling (171)" section on page 10-162.

Table 10-152 Signaling (171) Details

Description	Residential Gateway Unreachable
Severity	Minor
Threshold	100
Throttle	0
Datawords	Entity Name—STRING [40] General Context—STRING [40] Specific Context—STRING [40] Failure Context—STRING [40]
Primary Cause	An MGCP signaling interop error has occurred with the residential media gateway.
Primary Action	Check the IP connectivity status between Cisco BTS 10200 call agent and the trunking gateway. Check to see if the residential gateway is not physically connected, but controlled INS at the Cisco BTS 10200.

Signaling (172)

Table 10-153 lists the details of the Signaling (172) major alarm. To troubleshoot and correct the cause of the alarm, refer to the "Multimedia Terminal Adapter Effective-Aggr-Id Becomes Unavailable Due to Its IP Address—Signaling (172)" section on page 10-162.

Table 10-153 Signaling (172) Details

Description	Multimedia Terminal Adapter Effective-Aggr-Id Becomes Unavailable Due to its IP Address (MTA Effective-Aggr-Id Becomes Unavailable Due to its IP Address)
Severity	Major
Threshold	100
Throttle	0
Datawords	MTA IP Address—STRING [64]
Primary Cause	The MTA has been moved to a new subnet which is not provisioned, or provisioned with the aggr-id=null.
Primary Action	Provision the subnet aggr-id for the MTA.

Signaling (173)

Table 10-154 lists the details of the Signaling (173) critical alarm. To troubleshoot and correct the cause of the alarm, refer to the "ENUM Server Domain Cannot be Resolved Into Any IP Address —Signaling (173)" section on page 10-162.

Table 10-154 Signaling (173) Details

Description	ENUM Server Domain Cannot be Resolved into Any IP Address
Severity	Critical
Threshold	100
Throttle	0
Datawords	ENUM Server Domain - STRING [128] ENUM Profile ID - STRING [64]
Primary Cause	Misconfiguration in the DNS.
Primary Action	Fix the configuration in the DNS according to the documentation.

Signaling (174)

Table 10-155 lists the details of the Signaling (174) critical alarm. To troubleshoot and correct the cause of the alarm, refer to the "ENUM Server Unavailable—Signaling (174)" section on page 10-162.

Table 10-155 Signaling (174) Details

Description	ENUM Server Unavailable
Severity	Critical
Threshold	100
Throttle	0
Datawords	ENUM Server IP Address - STRING [16] ENUM Server Farm Name - STRING [128] ENUM Profile ID - STRING [64]
Primary Cause	A network or server problem has occurred.
Primary Action	Fix the network or server problem.

Signaling (175)

Table 10-156 lists the details of the Signaling (175) critical alarm. To troubleshoot and correct the cause of the alarm, refer to the "ENUM Server Farm Unavailable—Signaling (175)" section on page 10-163.

Table 10-156 Signaling (175) Details

Description	ENUM Server Farm Unavailable
Severity	Critical
Threshold	100
Throttle	0
Datawords	ENUM Server Farm Name - STRING [128] ENUM Profile ID - STRING [64]
Primary Cause	A network or server problem has occurred.
Primary Action	Fix the network or server problem.

Signaling (176)

Table 10-157 lists the details of the Signaling (176) critical alarm. To troubleshoot and correct the cause of the alarm, refer to the "No Resources Available to Launch ENUM Query—Signaling (176)" section on page 10-163.

Table 10-157 Signaling (176) Details

Description	No Resources Available to Launch ENUM Query
Severity	Critical
Threshold	100
Throttle	0
Datawords	
Primary Cause	Internal or network congestion or slow server response has occurred.
Primary Action	Fix the network congestion or improve the server response.

Signaling (177)

Table 10-158 lists the details of the Signaling (177) warning event. To monitor and correct the cause of the event, refer to the "ISDN Unable to Restore D-Channel Into In-Service Active State—Signaling (177)" section on page 10-131.

Table 10-158 Signaling (177) Details

Description	ISDN Unable to Restore D-Channel into In-Service Active State
Severity	Warning
Threshold	100
Throttle	0
Datawords	D-Chan ID - STRING [20] D-Chan Index - FOUR_BYTES D-Chan Type - STRING [10]
Primary Cause	The Cisco BTS 10200 does not receive the Service Ack from the remote end in response to Service message to make the D-Channel active.
Primary Action	Verify that the NFAS provisioning at the PBX/media gateway is correct.

Signaling (178)

Table 10-159 lists the details of the Signaling (178) informational event. For additional information, refer to the "Possible Overlap Dialing Misconfiguration—Signaling (178)" section on page 132.

Table 10-159 Signaling (178) Details

Description	Possible Overlap Dialing Misconfiguration
Severity	Information
Threshold	100
Throttle	0
Datawords	TGN-ID - FOUR_BYTES DIALED-DIGIT - STRING [20]
Primary Cause	The Cisco BTS 10200 sent out an invite with an overlap flag, and has received one or more additional digits to be forwarded. However, the call attempt fails while the Cisco BTS 10200 is still waiting to send out the first additional digit. A possible cause is a misconfiguration of the Overlap Dialing feature between the local and peer switch.
Primary Action	Make sure that the peer switch is configured to support the Overlap Dialing feature. Check that the feature is enabled and that the dial-plan is configured correctly. Also make sure that the Destination/Route/Trunk group on the peer switch is marked to support the Overlap Sending feature.

Signaling (179)

Table 10-160 lists the details of the Signaling (179) major alarm. To troubleshoot and correct the cause of the alarm, refer to the "Trunk Group Registration Expired—Signaling (179)" section on page 10-163.

Table 10-160 Signaling (179) Details

Description	Trunk Group Registration Expired
Severity	Major
Threshold	100
Throttle	0
Datawords	TGN-ID - FOUR_BYTES SIP Reg Contact - STRING [256] Reg Expiry Time - STRING [32]
Primary Cause	The trunk group did not register in time before the contact expiry.
Primary Action	The receipt of a subsequent registration will clear the alarm.

Signaling (182)

Table 10-161 lists the details of the Signaling (182) major alarm. To troubleshoot and correct the cause of the alarm, refer to the "Transient Issue Occurred on the Emergency End-points—Signaling (182)" section on page 10-163.

Table 10-161 Signaling (182) Details

Description	Transient Issue Occurred on the Emergency End-points
Severity	Major
Threshold	100
Throttle	0
Datawords	Endpoint-Name or Calling party—STRING[8]; (If available, otherwise is blank) Mgw-Name or Called party—STRING[8]; (If available, otherwise is blank) Error-description (in brief)—STRING[8]; (If available, otherwise is blank) Detailed error description—STRING[8]
Primary Cause	A transient error such as, 5XX error for CRCX, or a transient shm error, or an out-of-sequence message received at the MGA (MGCP protocol adapter) occurred on emergency end-points. Additionally, an error occurred for 911 call at BCM (Basic Call Module) such as trunk group OOS. This behavior is controlled by a new CA_CONFIG type —SPECIAL-ALARM-FOR-911-TRANS-ISSUES DATATYPE. The default value of this field is N. Set it to Y to enable logging of Signaling (182). For more information on the primary cause, see the "Transient Issue Occurred on the Emergency End-points—Signaling (182)" section on page 10-163.
Primary Action	Take action based on the description provided when the alarm is logged. For example, If the description indicates that the trunk is OOS, control the trunk back to INS, if required. Since these alarms only denote a transient error and do not have any corresponding trigger point to clear the alarm, the operator needs to clear the alarms from the CLI frequently (if the operator has opted for logging of this alarm).

Monitoring Signaling Events

This section provides the information you need for monitoring and correcting signaling events. Table 10-162 lists all of the signaling events in numerical order and provides cross-references to each subsection.

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

Table 10-162 Cisco BTS 10200 Signaling Events

Event Type	Event Name	Event Severity
Signaling (1)	Test Report—Signaling (1)	Information
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 Message—Signaling (25)	Warning
Signaling (26)	Unanswered Unblocking Message—Signaling (26)	Warning
Signaling (27)	Unanswered Circuit Group Blocking Message—Signaling (27)	Warning

Table 10-162 Cisco BTS 10200 Signaling Events (continued)

Event Type	Event Name	Event Severity
Signaling (28)	Unanswered Circuit Group Unblocking Message—Signaling (28)	Warning
Signaling (29)	Unanswered Circuit Query Message—Signaling (29)	Warning
Signaling (30)	Unanswered Circuit Validation Test Message—Signaling (30)	Warning
Signaling (31)	Unanswered Reset Circuit Message—Signaling (31)	Warning
Signaling (32)	Unanswered Group Reset Message—Signaling (32)	Warning
Signaling (33)	Unanswered Release Message—Signaling (33)	Warning
Signaling (34)	Unanswered Continuity Check Request Message—Signaling (34)	Warning
Signaling (36)	Trunk Locally Blocked—Signaling (36)	Minor
Signaling (40)	Trunk Remotely Blocked—Signaling (40)	Major
Signaling (42)	Continuity Testing Message Received on the Specified Circuit Identification Code—Signaling (42)	Information
Signaling (43)	Release Complete Received in Response to Reset Circuit Message on the Specified Circuit Identification Code—Signaling (43)	Information
Signaling (44)	Continuity Recheck Is Performed on Specified Circuit Identification Code—Signaling (44)	Information
Signaling (45)	Circuit Is Unequipped on Remote Side—Signaling (45)	Information
Signaling (46)	Specified Circuit Identification Code Is Invalid for the Operation—Signaling (46)	Information
Signaling (49)	A General Processing Error Encountered—Signaling (49)	Information
Signaling (50)	Unexpected Message for the Call State Is Received: Clear Call—Signaling (50)	Information
Signaling (51)	Set Trunk State as Remotely Unequipped—Signaling (51)	Information
Signaling (52)	Set Trunk State as Not Remotely Blocked—Signaling (52)	Information
Signaling (53)	Set Trunk State as Remotely Blocked—Signaling (53)	Information
Signaling (54)	Circuit Validation Test Aborted—Signaling (54)	Information
Signaling (55)	Circuit Validation Successful—Signaling (55)	Information
Signaling (57)	Continuity Recheck Failed—Signaling (57)	Information
Signaling (58)	Continuity Recheck Successful—Signaling (58)	Information
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)	Information
Signaling (62)	Received Integrated Services Digital Network Restart Message—Signaling (62)	Information

Table 10-162 Cisco BTS 10200 Signaling Events (continued)

Event Type	Event Name	Event Severity
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 (69)	Call Agent Is Not Up or Is Not Responding to the Feature Server—Signaling (69)	Critical
Signaling (70)	Integrated Services Digital Network Unable to Restore D-channel Due to Failed Communication—Signaling (70)	Warning
Signaling (71)	Integrated Services Digital Network Unable to Establish D-Channel—Signaling (71)	Warning
Signaling (72)	Integrated Services Digital Network—Calls Lost Due to D-Channel Down for Period of Time—Signaling (72)	Warning
Signaling (73)	Integrated Services Digital Network—Unable to Send Restart Due to Restart Timer Expired—Signaling (73)	Warning
Signaling (74)	Integrated Services Digital Network: Unable to Send the Service Due to the Service Timer Expired—Signaling (74)	Warning
Signaling (75)	Signaling System 7 Stack Not Ready—Signaling (75)	Critical
Signaling (76)	Timeout on Remote Instance—Signaling (76)	Information
Signaling (77)	Integrated Services Digital Network D-Channel Switchover for Not Facility Associated Signaling—Signaling (77)	Information
Signaling (78)	Integrated Services Digital Network Single D-Channel Down for Not Facility Associated Signaling—Signaling (78)	Minor
Signaling (79)	Trunking Gateway Unreachable—Signaling (79)	Major
Signaling (80)	Out of Bounds, Memory/Socket Error—Signaling (80)	Critical
Signaling (81)	Insufficient Heap Memory—Signaling (81)	Critical
Signaling (82)	Insufficient Shared Memory Pools—Signaling (82)	Critical
Signaling (83)	Error While Binding to Socket—Signaling (83)	Critical
Signaling (84)	Reached Maximum Socket Limit—Signaling (84)	Critical
Signaling (85)	Initialization Failure—Signaling (85)	Critical
Signaling (86)	Remote H.323 Gateway Is Not Reachable—Signaling (86)	Major
Signaling (87)	H.323 Message Parsing Error—Signaling (87)	Major
Signaling (88)	H.323 Message Encoding Error—Signaling (88)	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)	Major
Signaling (92)	Invalid Call Identifier—Signaling (92)	Minor

Table 10-162 Cisco BTS 10200 Signaling Events (continued)

Event Type	Event Name	Event Severity
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)	H.323 Protocol Inconsistencies—Signaling (98)	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)	H.323 Network Congested—Signaling (102)	Minor
Signaling (103)	Aggregation Connection Down—Signaling (103)	Major
Signaling (104)	Aggregation Unable to Establish Connection—Signaling (104)	Information
Signaling (105)	Aggregation Gate Set Failed—Signaling (105)	Information
Signaling (106)	Enhanced Subscriber Authentication Cisco BTS 10200 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 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

Table 10-162 Cisco BTS 10200 Signaling Events (continued)

Event Type	Event Name	Event Severity
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)	Information
Signaling (134)	Signaling System 7 Message Encoding Failure—Signaling (134)	Information
Signaling (135)	Signaling System 7 Message Decoding Failure—Signaling (135)	Information
Signaling (136)	Signaling System 7 Message Invalid Received—Signaling (136)	Information
Signaling (137)	Signaling System 7 Confusion Message Received—Signaling (137)	Information
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)	Information
Signaling (140)	Unanswered Information Message—Signaling (140)	Information
Signaling (141)	Address Not Resolved by Domain Name System Server—Signaling (141)	Warning
Signaling (142)	Session Initiation Protocol Trunk Operationally Out-of-Service—Signaling (142)	Critical
Signaling (143)	Internet Protocol Interface Link to the Signaling System 7 Signaling Gateway Is Down—Signaling (143)	Minor
Signaling (144)	All Internet Interface Links to Signaling System 7 Signaling Gateway Are Down—Signaling (144)	Critical
Signaling (145)	One Internet Protocol Interface to Signaling System 7 Signaling Gateway Is Down—Signaling (145)	Minor
Signaling (146)	All Retransmission Attempts of Session Initiation Protocol Request or Response Failed—Signaling (146)	Warning

Table 10-162 Cisco BTS 10200 Signaling Events (continued)

Event Type	Event Name	Event Severity
Signaling (147)	Domain Name System Service Addresses Exhausted—Signaling (147)	Warning
Signaling (150)	Stream Control Transmission Protocol Association Congested—Signaling (150)	Minor
Signaling (151)	Subscriber Line Faulty—Signaling (151)	Minor
Signaling (152)	Termination Transient Error Received—Signaling (152)	Information
Signaling (153)	Emergency Trunks Become Locally Blocked—Signaling (153)	Critical
Signaling (154)	Emergency Trunks Become Remotely Blocked—Signaling (154)	Critical
Signaling (155)	Packet Cable Multi-Media Unsolicited Gate Delete—Signaling (155)	Information
Signaling (156)	Integrated Services Digital Network Signaling Gateway Down—Signaling (156)	Major
Signaling (157)	Integrated Services Digital Network Signaling Gateway Inactive—Signaling (157)	Major
Signaling (158)	Invalid Integrated Services Digital Network Interface Identification—Signaling (158)	Warning
Signaling (159)	Integrated Services Digital Network User Adaptation Layer Cannot Go Active—Signaling (159)	Warning
Signaling (160)	Integrated Services Digital Network User Adaptation Layer Cannot Go Standby—Signaling (160)	Warning
Signaling (161)	Session Initiation Protocol Update Not Allowed for Operator Service Position System Calls—Signaling (161)	Warning
Signaling (162)	Session Initiation Protocol Server Group Element Operationally Out of Service—Signaling (162)	Critical
Signaling (163)	Routing Key Inactive—Signaling (163)	Major
Signaling (164)	Signaling Gateway Traffic Mode Mismatch—Signaling (164)	Major
Signaling (165)	No Session Initiation Protocol P-DCS Billing Information Header Received—Signaling (165)	Warning
Signaling (166)	No Routing Keys Are Active—Signaling (166)	Warning
Signaling (167)	No Signaling Gateways Are Active—Signaling (167)	Warning
Signaling (168)	A Session Initiation Protocol Server Group Has No Child Elements Provisioned—Signaling (168)	Warning
Signaling (169)	Session Initiation Protocol Element Provisioned With Service Enabled Is Internally Disabled—Signaling (169)	Information
Signaling (170)	Residential Gateway Endpoints Are Out of Service at the Gateway—Signaling (170)	Minor
Signaling (171)	Residential Gateway Unreachable—Signaling (171)	Minor
Signaling (172)	Multimedia Terminal Adapter Effective-Aggr-Id Becomes Unavailable Due to Its IP Address—Signaling (172)	Major

Table 10-162 Cisco BTS 10200 Signaling Events (continued)

Event Type	Event Name	Event Severity
Signaling (173)	ENUM Server Domain Cannot be Resolved Into Any IP Address —Signaling (173)	Critical
Signaling (174)	ENUM Server Unavailable—Signaling (174)	Critical
Signaling (175)	ENUM Server Farm Unavailable—Signaling (175)	Critical
Signaling (176)	No Resources Available to Launch ENUM Query—Signaling (176)	Critical
Signaling (177)	ISDN Unable to Restore D-Channel Into In-Service Active State—Signaling (177)	Warning
Signaling (178)	Possible Overlap Dialing Misconfiguration—Signaling (178)	Information
Signaling (179)	Trunk Group Registration Expired—Signaling (179)	Major
Signaling (182)	Transient Issue Occurred on the Emergency End-points—Signaling (182)	Major

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 reprovisioned.

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 10-136.

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 10-137.

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 10-137.

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 10-138.

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 10-138.

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 10-138.

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 10-138.

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 10-139.

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 10-139.

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 10-139.

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 10-139.

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 10-139.

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 10-139.

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 10-140.

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 10-140.

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 10-140.

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 10-141.

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 10-142.

Unanswered Blocking Message—Signaling (25)

The Unanswered Blocking Message event serves as a warning that a BLO message was not answered. The primary cause of the event is that a BLO message was not acknowledged before the T13 expired for the associated CIC. To correct the primary cause of the event, verify that:

- The SS7 signaling adapter processes are running normally.
- The call agent platform is active.
- The SS7 interface hardware is in service.
- The associated SS7 signaling link is available.
- The T13 timer is set to an appropriate level.T
- he 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 are running normally.
- The call agent platform is active.
- The SS7 interface hardware is in service.
- The associated SS7 signaling link is available.
- The T13 timer is set to an appropriate level.
- The SS7 link is not congested.

Unanswered Circuit Group Blocking Message—Signaling (27)

The Unanswered Circuit Group Blocking Message event serves as a warning that a CGB message was not answered. The primary cause of the event is that a CGB message was not acknowledged before the T19 expired for the associated CIC. To correct the primary cause of the event, verify that:

- The SS7 signaling adapter processes are running normally.
- The call agent platform is active.
- The SS7 interface hardware is in service.
- The associated SS7 signaling link is available.
- The T13 timer is set to an appropriate level.
- The SS7 link is not congested.

Unanswered Circuit Group Unblocking Message—Signaling (28)

The Unanswered Circuit Group Unblocking Message event serves as a warning that a CGU message was not answered. The primary cause of the event is that a CGU message was not acknowledged before the T21 expired for the associated CIC. To correct the primary cause of the event, verify that:

- The SS7 signaling adapter processes are running normally.
- The call agent platform is active.
- The SS7 interface hardware is in service.
- The associated SS7 signaling link is available.
- The T13 timer is set to an appropriate level.
- 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 are running normally.
- The call agent platform is active.
- The SS7 interface hardware is in service.
- The associated SS7 signaling link is available.
- The T13 timer is set to an appropriate level.
- The SS7 link is not congested.

Unanswered Circuit Validation Test Message—Signaling (30)

The Unanswered Circuit Validation Test Message event serves as a warning that a CVT message was not answered. The primary cause of the event is that a CVT message was not acknowledged before the Tcvt expired for the associated CIC. To correct the primary cause of the event, verify that:

- The SS7 signaling adapter processes are running normally.
- The call agent platform is active.
- The SS7 interface hardware is in service.
- The associated SS7 signaling link is available.
- The T13 timer is set to an appropriate level.
- The SS7 link is not congested.

Unanswered Reset Circuit Message—Signaling (31)

The Unanswered Reset Circuit Message event serves as a warning that an 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 are running normally.

The call agent platform is active.

The SS7 interface hardware is in service.

The associated SS7 signaling link is available.

The T13 timer is set to an appropriate level.

The SS7 link is not congested.

Unanswered Group Reset Message—Signaling (32)

The Unanswered Group Reset Message event serves as a warning that a GRS message was not answered. The primary cause of the event is that a 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.
- The call agent platform is active.
- The SS7 interface hardware is in service.
- The associated SS7 signaling link is available.
- The T13 timer is set to an appropriate level.
- The SS7 link is not congested.

Unanswered Release Message—Signaling (33)

The Unanswered Release Message event serves as a warning that an 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 are running normally.
- The call agent platform is active.
- The SS7 interface hardware is in service.
- The associated SS7 signaling link is available.
- The T13 timer is set to an appropriate level.
- The SS7 link is not congested.

Unanswered Continuity Check Request Message—Signaling (34)

The Unanswered Continuity Check Request Message event serves as a warning that a continuity check request (CCR) message was not answered. The primary cause of the event is that an 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 are running normally.
- The call agent platform is active.
- The SS7 interface hardware is in service.
- The associated SS7 signaling link is available.
- The T13 timer is set to an appropriate level.
- 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 10-142.

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 10-142.

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 no 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 indicating that 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 find out whether an existing circuit was unequipped causing a status mismatch with the local end.

Specified Circuit Identification Code Is Invalid for the Operation—Signaling (46)

The Specified Circuit Identification Code Is Invalid for the Operation event functions as an informational alert that the specified CIC is invalid for the attempted operation. The primary cause of the event is that an invalid operation was performed on the specified CIC. To correct the primary cause of the event, verify that the SS7 provisioning tables are properly configured at the circuit level.

A General Processing Error Encountered—Signaling (49)

The A General Processing Error Encountered event functions as an informational alert that a general processing error has occurred. The primary cause of the event is that a general SS7 processing error occurred because all resources were busy or because an invalid even occurred. To correct the primary cause of the event, check the status of the signaling adapter process and the SS7 signaling interface to verify proper operation.

Unexpected Message for the Call State Is Received: Clear Call—Signaling (50)

The Unexpected Message for the Call State Is Received: Clear Call event functions as an informational alert that an unexpected message for the call state has been received. The primary cause of the event is that an unexpected message was received for the current call state. To correct the primary cause of the event, examine the status of the signaling adapter process and the SS7 signaling interface to verify proper operation.

Set Trunk State as Remotely Unequipped—Signaling (51)

The Set Trunk State as Remotely Unequipped event functions as an informational alert that the trunk state is currently set as remotely unequipped. The primary cause of the event is that the specified CIC is marked as remotely unequipped due to the CQM response indicating that it is unequipped at the far end. To correct the primary cause of the event, equip the trunk circuit at the far end.

Set Trunk State as Not Remotely Blocked—Signaling (52)

The Set Trunk State as Not Remotely Blocked event functions as an informational alert that the trunk state has been set as not remotely blocked. The primary cause of the event is that the specified CIC is marked as not remotely blocked due to the CQM response indicating that it is not remotely blocked at the far end. The event is informational and no further action is required.

Set Trunk State as Remotely Blocked—Signaling (53)

The Set Trunk State as Remotely Blocked event functions as an informational alert that the trunk state is set as remotely blocked. The primary cause of the event is that the specified CIC is marked as remotely blocked due to the CQM response indicating that it is remotely blocked at the far end. To correct the primary cause of the event, clear the blocking situation at the far end based on network level event reports.

Circuit Validation Test Aborted—Signaling (54)

The Circuit Validation Test Aborted event functions as an informational alert that the circuit validation test has been aborted. The primary cause of the event is that the circuit specified failed a validation test due to an internal failure. To correct the primary cause of the event, verify that 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 that the SS7 signaling adapter process and the SS7 interface are 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 a 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 10-142.

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 by 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, an unknown package type, an 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 10-142.

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 10-143.

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 10-143.

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 10-143.

Call Agent Is Not Up or Is Not Responding to the Feature Server—Signaling (69)

The Call Agent Is Not Up or Is Not Responding to the Feature Server alarm (critical) indicates that a CA and FS communications message timed out. To troubleshoot and correct the cause of the Call Agent Is Not Up or Is Not Responding to the Feature Server alarm, refer to the "Call Agent Is Not Up or Is Not Responding to the Feature Server—Signaling (69)" section on page 10-143.

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 troubleshoot 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 10-143.

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 Not Facility Associated Signaling—Signaling (77)

The Integrated Services Digital Network D-Channel Switchover for Not Facility Associated Signaling event functions as an informational alert that an ISDN D-channel switchover has occurred for 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 the gateway is operational and connection to PBX is good.

Integrated Services Digital Network Single D-Channel Down for Not Facility Associated Signaling—Signaling (78)

The Integrated Services Digital Network Single D-Channel Down for Not 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 Not Facility Associated Signaling alarm, refer to the "Integrated Services Digital Network Single D-Channel Down for Not Facility Associated Signaling—Signaling (78)" section on page 10-144.

Trunking Gateway Unreachable—Signaling (79)

The Trunking Gateway Unreachable alarm (major) indicates that the trunking gateway is not responding to keep-alive Audit Endpoint messages. To troubleshoot and correct the cause of the Media Gateway Unreachable alarm, refer to the "Trunking Gateway Unreachable—Signaling (79)" section on page 10-144.

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 10-144.

Insufficient Heap Memory—Signaling (81)

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)" section on page 10-144.

Insufficient Shared Memory Pools—Signaling (82)

The Insufficient Shared Memory Pools alarm (critical) indicates that there are 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)" section on page 10-144.

Error While Binding to Socket—Signaling (83)

The Error While Binding to Socket alarm (critical) indicates that an error occurred while the system was 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 10-145.

Reached Maximum Socket Limit—Signaling (84)

The Reached Maximum Socket Limit alarm (critical) indicates that the Cisco BTS 10200 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)" section on page 10-145.

Initialization Failure—Signaling (85)

The Initialization Failure alarm (critical) indicates that the Cisco BTS 10200 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 10-145.

Remote H.323 Gateway Is Not Reachable—Signaling (86)

The Remote H.323 Gateway Is Not Reachable alarm (major) indicates that the remote H.323 gateway is not reachable. To troubleshoot and correct the cause of the Remote H.323 Gateway Is Not Reachable alarm, refer to the "Remote H.323 Gateway Is Not Reachable—Signaling (86)" section on page 10-145.

H.323 Message Parsing Error—Signaling (87)

The H.323 Message Parsing Error alarm (major) indicates that a H.323 message-parsing error has occurred. To troubleshoot and correct the cause of the H.323 Message Parsing Error alarm, refer to the "H.323 Message Parsing Error—Signaling (87)" section on page 10-145.

H.323 Message Encoding Error—Signaling (88)

The H.323 Message Encoding Error alarm (major) indicates that a H.323 message-encoding error has occurred. To troubleshoot and correct the cause of the H.323 Message Encoding Error alarm, refer to the "H.323 Message Encoding Error—Signaling (88)" section on page 10-145.

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 10-146.

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 10-146.

Endpoint Security Violation—Signaling (91)

The Endpoint Security Violation alarm (major) indicates that an H.323 security violation has occurred. To troubleshoot and correct the cause of the Endpoint Security Violation alarm, refer to the "Endpoint Security Violation—Signaling (91)" section on page 10-146.

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 10-146.

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 10-146.

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 10-146.

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 10-147.

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 10-147.

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 10-147.

H.323 Protocol Inconsistencies—Signaling (98)

The H.323 Protocol Inconsistencies alarm (minor) indicates that the H.323 endpoint and Cisco BTS 10200 are running different protocol versions. To troubleshoot and correct the cause of the H.323 Protocol Inconsistencies alarm, refer to the "H.323 Protocol Inconsistencies—Signaling (98)" section on page 10-147.

Abnormal Call Clearing—Signaling (99)

The Abnormal Call Clearing alarm (minor) indicates that an unsupported or invalid message type was received from the network. To troubleshoot and correct the cause of the Abnormal Call Clearing alarm, refer to the "Abnormal Call Clearing—Signaling (99)" section on page 10-147.

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 10-147.

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 10-147.

H.323 Network Congested—Signaling (102)

The H.323 Network Congested alarm indicates (minor) that the H.323 application process has depleted its resources and no more calls can be completed. To troubleshoot and correct the cause of the H.323 Network Congested alarm, refer to the "H.323 Network Congested—Signaling (102)" section on page 10-148.

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 10-148.

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 Delivery Function Connection Down—Signaling (106)

The Enhanced Subscriber Authentication Cisco BTS 10200 Delivery Function Connection Down alarm (minor) indicates that the enhanced subscriber authentication (ESA) Cisco BTS 10200 DF connection is down. To troubleshoot and correct the cause of the Enhanced Subscriber Authentication Cisco BTS 10200 Delivery Function Connection Down alarm, refer to the "Enhanced Subscriber Authentication Cisco BTS 10200 Delivery Function Connection Down—Signaling (106)" section on page 10-148.

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 10-148.

Simplex Only Operational Mode—Signaling (108)

The Simplex Only Operational Mode alarm (major) indicates that the Cisco BTS 10200 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 10-148.

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 10-149.

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 10-152.

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 10-153.

Stream Control Transmission Protocol Association Configuration Error—Signaling (112)

The Stream Control Transmission Protocol Association Configuration Error alarm (minor) indicates that an 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 10-154.

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 10-155.

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 10-155.

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 10-156.

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 10-156.

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 10-156.

Signaling System 7 Adapter Process Faulty—Signaling (119)

The Signaling System 7 Adapter Process Faulty alarm (critical) indicates that an S7A process is faulty. To troubleshoot and correct the cause of the Signaling System 7 Adapter Process Faulty alarm, refer to the "Signaling System 7 Adapter Process Faulty—Signaling (119)" section on page 10-156.

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 "Signaling System 7 Module/Signaling System 7 Adapter Faulty—Signaling (120)" section on page 10-156.

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 10-157.

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 10-157.

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 10-157.

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 10-157.

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 10-158.

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 10-158.

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 preconfigured dialogue IDs or invoke IDs. To correct the primary cause of the event, increase the number of preconfigured 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 an 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.

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 an 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 an SS7 trace of the circuit for examination by Cisco TAC.

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 an SS7 trace of the circuit for examination by Cisco TAC.

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 an 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.

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, 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 the limit.

Signaling System 7 Trunk was Found to be in Erroneous State—Signaling (139)

The Signaling System 7 Trunk was Found to be in Erroneous State event functions as an informational alert that an 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 by use of the 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 an 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 provisioning.

The following tips might help you troubleshoot NLP/DNS related issues:

- Grep for GET_HOST_BY_NAME keyword in the traces at INFO3 trace level.
- Grep for warning/error keyword in the traces at INFO3 trace level.

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 10-158.

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 10-158.

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 10-158.

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 10-159.

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 that 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 correct the order of IP addresses and ensure that previous hop network component is alive and in a healthy state.

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 provisioning.

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 10-159.

Subscriber Line Faulty—Signaling (151)

The Subscriber Line Faulty alarm (minor) indicates that the residential gateway returned an error code in response to a command from the MGW. To troubleshoot and correct the cause of the Subscriber Line Faulty alarm, refer to the "Subscriber Line Faulty—Signaling (151)" section on page 10-160.

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 is that the MGCP signaling process has inter-operational errors. To correct the primary cause of the event, notify Cisco TAC.

Emergency Trunks Become Locally Blocked—Signaling (153)

The Emergency Trunks Become Locally Blocked alarm (critical) indicates that an emergency trunk (CAS, SS7, or ISDN) is locally blocked. To troubleshoot and correct the cause of the Emergency Trunks Become Locally Blocked alarm, refer to the "Emergency Trunks Become Locally Blocked—Signaling (153)" section on page 10-160.

Emergency Trunks Become Remotely Blocked—Signaling (154)

The Emergency Trunks Become Remotely Blocked alarm (critical) indicates that an emergency trunk (CAS, SS7, or ISDN) is remotely blocked. To troubleshoot and correct the cause of the Emergency Trunks Become Remotely Blocked alarm, refer to the "Emergency Trunks Become Remotely Blocked—Signaling (154)" section on page 10-160.

Packet Cable Multi-Media Unsolicited Gate Delete—Signaling (155)

The Packet Cable Multi-Media Unsolicited Gate Delete event serves as an informational alert that an error condition was encountered by the CMTS. To correct the cause of the event, check the alarms and warnings from the CMTS.

Integrated Services Digital Network Signaling Gateway Down—Signaling (156)

The Integrated Services Digital Network Signaling Gateway Down alarm (major) indicates that the Cisco BTS 10200 system cannot communicate with the ISDN gateway. To troubleshoot and correct the cause of the Integrated Services Digital Network Signaling Gateway Down alarm, refer to the "Integrated Services Digital Network Signaling Gateway Down—Signaling (156)" section on page 10-161.

Integrated Services Digital Network Signaling Gateway Inactive—Signaling (157)

The Integrated Services Digital Network Signaling Gateway Inactive alarm (major) indicates that a **shutdown** command has been executed in the application server on the ISDN gateway side. To troubleshoot and correct the cause of the Integrated Services Digital Network Signaling Gateway Inactive alarm, refer to the "Integrated Services Digital Network Signaling Gateway Inactive—Signaling (157)" section on page 10-161.

Invalid Integrated Services Digital Network Interface Identification—Signaling (158)

The Invalid Integrated Services Digital Network Interface Identification event serves as a warning that an interface ID is not configured correctly on the ISDN gateway side. To correct the cause of the event, configure the D-channel correctly on the gateway side. The D-channel configuration on the call-agent side should match that on the gateway side.

Integrated Services Digital Network User Adaptation Layer Cannot Go Active—Signaling (159)

The Integrated Services Digital Network User Adaptation Layer Cannot Go Active event serves as a warning that no active acknowledgement messages are being received from any signaling gateway. This indicates that the ISDN signaling gateway or the SCTP associations are probably down. To correct the cause of the event, investigate other alarms to see if the signaling gateways are down or to see if the SCTP associations are down. Take corrective action according to the alarm indications.

Integrated Services Digital Network User Adaptation Layer Cannot Go Standby—Signaling (160)

The Integrated Services Digital Network User Adaptation Layer Cannot Go Standby event serves as a warning that no active acknowledgement messages are being received from any signaling gateway. This indicates that the ISDN signaling gateway or the SCTP associations are probably down. To correct the cause of the event, investigate other alarms to see if the signaling gateways are down or the SCTP associations are down. Take corrective action according to the alarm indications.

Session Initiation Protocol Update Not Allowed for Operator Service Position System Calls—Signaling (161)

The Session Initiation Protocol Update Not Allowed for Operator Service Position System Calls event serves as a warning that the remote switch is not allowing the Cisco BTS 10200 to send SIP update messages. The update messages are mandatory in the CMSS and are used exclusively by the Cisco BTS 10200 for operator service calls over SIP including BLV, emergency interrupt, and 911 ringback calls. To correct the cause of the event, upgrade or reprovision the remote switch so it can process incoming SIP update messages.

Session Initiation Protocol Server Group Element Operationally Out of Service—Signaling (162)

The Session Initiation Protocol Server Group Element Operationally Out of Service alarm (critical) indicates that the Cisco BTS 10200 is unable to communicate with a remote SIP party (call-agent or proxy) over a SIP server group element. To troubleshoot and correct the cause of the Session Initiation Protocol Server Group Element Operationally Out of Service alarm, refer to the "Session Initiation Protocol Server Group Element Operationally Out of Service—Signaling (162)" section on page 10-161.

Routing Key Inactive—Signaling (163)

The Routing Key Inactive alarm (major) indicates that inactive acknowledgement messages were received from a Signaling Gateway. The SG or SCTP associations are probably down. To troubleshoot and correct the primary cause of the Routing Key Inactive alarm, refer to the "Routing Key Inactive—Signaling (163)" section on page 10-161.

Signaling Gateway Traffic Mode Mismatch—Signaling (164)

The Signaling Gateway Traffic Mode Mismatch alarm (major) indicates that the traffic mode does not match on the Cisco BTS 10200 and the Signaling Gateway. To troubleshoot and correct the primary cause of the Signaling Gateway Traffic Mode Mismatch alarm, refer to the "Signaling Gateway Traffic Mode Mismatch—Signaling (164)" section on page 10-162.

No Session Initiation Protocol P-DCS Billing Information Header Received—Signaling (165)

The No Session Initiation Protocol P-DCS Billing Information Header Received event serves as a warning that no SIP P-DCS billing information headers are being received. The primary cause of the event is that the originating switch is not provisioned to add the P-DCS Billing Information header to outgoing SIP requests and responses. To correct the primary cause of the event, provision the originating switch to add P-DCS Billing Information header to outgoing messages. The secondary cause of the event is that the header could have been stripped off by an intermediate proxy. To correct the secondary cause of the event, determine if the header has been stripped off by an intermediate proxy and configure the system for corrective action if so. The ternary cause of the event is that there was a SIP message encoding error at the sending switch. To correct the ternary cause of the event, determine if a SIP message encoding error occurred at the adjacent switch and if so, call the technical assistance center to determine a fix for the problem.

No Routing Keys Are Active—Signaling (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. To correct the primary cause of the event, check the communication path between Cisco BTS 10200 and the ITP.

A Session Initiation Protocol Server Group Has No Child Elements Provisioned—Signaling (168)

The A Session Initiation Protocol Server Group Has No Child Elements Provisioned event is issued as a warning when a SIP Server Group administrative in-service is provisioned but has no child elements provisioned. This Server Group will be considered as if it were administratively out of service. If that is acceptable, no action is required. If the server group was expected to be workable, place the server group back out of service, resolve the provisioning problem, and place it back into service.

Session Initiation Protocol Element Provisioned With Service Enabled Is Internally Disabled—Signaling (169)

The Session Initiation Protocol Element Provisioned with Service Enabled is Internally Disabled event functions as an informational alert that a SIP element was provisioned with SRV enabled and is associated to at least one or more Server Groups. The SRV flag will be assumed disabled. However, to resolve this informational message, provision the SRV flag disabled on the SIP element.

Residential Gateway Endpoints Are Out of Service at the Gateway—Signaling (170)

The Residential Gateway Endpoints Are Out of Service at the Gateway alarm (minor) indicates that the residential gateway has been administratively taken OOS using the command at the gateway. To troubleshoot and correct the primary cause of the Residential Gateway Endpoints Are Out of Service at the Gateway alarm, refer to the "Residential Gateway Endpoints Are Out of Service at the Gateway—Signaling (170)" section on page 10-162.

Residential Gateway Unreachable—Signaling (171)

The Residential Gateway Unreachable alarm (minor) indicates that a MGCP signaling interop error has occurred with the residential media gateway. To troubleshoot and correct the primary cause of the Residential Gateway Unreachable alarm, refer to the "Residential Gateway Unreachable—Signaling (171)" section on page 10-162.

Multimedia Terminal Adapter Effective-Aggr-Id Becomes Unavailable Due to Its IP Address—Signaling (172)

The Multimedia Terminal Adapter Effective-Aggr-Id Becomes Unavailable Due to Its IP Address alarm (major) indicates that the MTA has been moved to a new subnet which is not provisioned, or provisioned with the aggr-id=null. To troubleshoot and correct the primary cause of the Multimedia Terminal Adapter Effective-Aggr-Id Becomes Unavailable Due to Its IP Address alarm, refer to the "Multimedia Terminal Adapter Effective-Aggr-Id Becomes Unavailable Due to Its IP Address—Signaling (172)" section on page 10-162.

ENUM Server Domain Cannot be Resolved Into Any IP Address —Signaling (173)

The ENUM Server Domain Cannot be Resolved Into Any IP Address alarm (critical) indicates that a misconfiguration has occurred in the DNS configuration. To troubleshoot and correct the cause of the ENUM Server Domain Cannot be Resolved Into Any IP Address alarm, refer to the "ENUM Server Domain Cannot be Resolved Into Any IP Address —Signaling (173)" section on page 10-162.

ENUM Server Unavailable—Signaling (174)

The ENUM Server Unavailable alarm (critical) indicates that a network or server problem has occurred. To troubleshoot and correct the cause of the ENUM Server Unavailable alarm, refer to the "ENUM Server Unavailable—Signaling (174)" section on page 10-162.

ENUM Server Farm Unavailable—Signaling (175)

The ENUM Server Farm Unavailable alarm (critical) indicates that a network or server problem has occurred. To troubleshoot and correct the cause of the ENUM Server Farm Unavailable alarm, refer to the "ENUM Server Farm Unavailable—Signaling (175)" section on page 10-163.

No Resources Available to Launch ENUM Query—Signaling (176)

The No Resources Available to Launch ENUM Query alarm (critical) indicates that no resources are available to launch the ENUM query. The primary cause of the alarm is that there is internal or network congestion or that the server response is slow. To troubleshoot and correct the primary cause of the alarm, refer to the "No Resources Available to Launch ENUM Query—Signaling (176)" section on page 10-163.

ISDN Unable to Restore D-Channel Into In-Service Active State—Signaling (177)

The ISDN Unable to Restore D-Channel Into In-Service Active State warning event indicates that the Cisco BTS 10200 did not receive the Service Ack from the remote end in response to the Service message to make the D-Channel active. To correct the cause of the event, ensure that the NFAS provisioning at the PBX/media gateway is correct.

Possible Overlap Dialing Misconfiguration—Signaling (178)

The Possible Overlap Dialing Misconfiguration event serves as an informational alert that the Cisco BTS 10200 sent out an invite with an overlap flag, and has received one or more additional digits to be forwarded. However, the call attempt fails while the Cisco BTS 10200 is still waiting to send out the first additional digit. A possible cause is a misconfiguration of the Overlap Dialing feature between the local and peer switches. To correct the cause of the event, make sure that the peer switch is configured to support the Overlap Dialing feature. Check that the feature is enabled and that the dial-plan is configured correctly. Also make sure that the Destination/Route/Trunk group on the peer switch is marked to support the Overlap Sending feature.

Trunk Group Registration Expired—Signaling (179)

The Trunk Group Registration Expired alarm (major) indicates that a trunk group registration has expired. The primary cause of the alarm is that the trunk group did not register in time before the contact expiry. To troubleshoot and correct the primary cause of the Trunk Group Registration Expired alarm, refer to the "Trunk Group Registration Expired—Signaling (179)" section on page 10-163.

Troubleshooting Signaling Alarms

This section provides the information you need for monitoring and correcting signaling alarms. Table 10-163 lists all of the signaling alarms in numerical order and provides cross-references to each subsection.

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

Table 10-163 Cisco BTS 10200 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

Table 10-163 Cisco BTS 10200 Signaling Alarms (continued)

Alarm Type	Alarm Name	Alarm Severity
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 (69)	Call Agent Is Not Up or Is Not Responding to the Feature Server—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 Not Facility Associated Signaling—Signaling (78)	Minor
Signaling (79)	Trunking Gateway Unreachable—Signaling (79)	Major
Signaling (80)	Out of Bounds, Memory/Socket Error—Signaling (80)	Critical
Signaling (81)	Insufficient Heap Memory—Signaling (81)	Critical
Signaling (82)	Insufficient Shared Memory Pools—Signaling (82)	Critical
Signaling (83)	Error While Binding to Socket—Signaling (83)	Critical
Signaling (84)	Reached Maximum Socket Limit—Signaling (84)	Critical
Signaling (85)	Initialization Failure—Signaling (85)	Critical
Signaling (86)	Remote H.323 Gateway Is Not Reachable—Signaling (86)	Major
Signaling (87)	H.323 Message Parsing Error—Signaling (87)	Major
Signaling (88)	H.323 Message Encoding Error—Signaling (88)	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)	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)	H.323 Protocol Inconsistencies—Signaling (98)	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)	H.323 Network Congested—Signaling (102)	Minor
Signaling (103)	Aggregation Connection Down—Signaling (103)	Major
Signaling (106)	Enhanced Subscriber Authentication Cisco BTS 10200 Delivery Function Connection Down—Signaling (106)	Minor
Signaling (107)	Logical Internet Protocol Addresses Not Mapped Correctly—Signaling (107)	Critical

Table 10-163 Cisco BTS 10200 Signaling Alarms (continued)

Alarm Type	Alarm Name	Alarm Severity
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
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)	Subscriber Line Faulty—Signaling (151)	Minor
Signaling (153)	Emergency Trunks Become Locally Blocked—Signaling (153)	Critical

Table 10-163 Cisco BTS 10200 Signaling Alarms (continued)

Alarm Type	Alarm Name	Alarm Severity
Signaling (154)	Emergency Trunks Become Remotely Blocked—Signaling (154)	Critical
Signaling (156)	Integrated Services Digital Network Signaling Gateway Down—Signaling (156)	Major
Signaling (157)	Integrated Services Digital Network Signaling Gateway Inactive—Signaling (157)	Major
Signaling (162)	Session Initiation Protocol Server Group Element Operationally Out of Service—Signaling (162)	Critical
Signaling (163)	Routing Key Inactive—Signaling (163)	Major
Signaling (164)	Signaling Gateway Traffic Mode Mismatch—Signaling (164)	Major
Signaling (170)	Residential Gateway Endpoints Are Out of Service at the Gateway—Signaling (170)	Minor
Signaling (171)	Residential Gateway Unreachable—Signaling (171)	Minor
Signaling (172)	Multimedia Terminal Adapter Effective-Aggr-Id Becomes Unavailable Due to Its IP Address—Signaling (172)	Major
Signaling (173)	ENUM Server Domain Cannot be Resolved Into Any IP Address —Signaling (173)	Critical
Signaling (174)	ENUM Server Unavailable—Signaling (174)	Critical
Signaling (175)	ENUM Server Farm Unavailable—Signaling (175)	Critical
Signaling (176)	No Resources Available to Launch ENUM Query—Signaling (176)	Critical
Signaling (179)	Trunk Group Registration Expired—Signaling (179)	Major

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 that 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.

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 might 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 might 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.

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 the **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 is unable to communicate with a gateway. Verify that the gateway is 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 resending 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.

Failed to Allocate Session Initiation Protocol Control Block—Signaling (11)

The Failed to Allocate Session Initiation Protocol Control Block alarm (major) indicates that a SIP control block allocation failed. The primary cause of the alarm is that there is not enough memory to allocate a SIP Call Control Block. To correct the primary cause of the alarm, Increase the SIP CCB count specified in mem.cfg file and restart the Call Agent for the changes to take effect.

Feature Server Is Not Up or Is Not Responding to Call Agent—Signaling (12)

The Feature Server Is Not Up or Is Not Responding to Call Agent alarm (critical) indicates that the feature server is not up or is not responding to the call agent server. The primary cause of the alarm is that the feature server platform is down or is not operating properly. To correct the primary cause of the alarm, restart the applicable feature server.

Signaling System 7 Signaling Link Down—Signaling (13)

The Signaling System 7 Signaling Link Down alarm (major) indicates the SS7 signaling link is down. The primary cause of the alarm is that the SS7 trunk group may be out-of-service (OOS). To correct the primary cause of the alarm, use the **control ss7-trunk-grp** command to place the trunk group in service (INS). The secondary cause of the alarm is that the local Ulticom stack may be down. To correct the secondary cause of the alarm, run the Ulticom **stack** command again. The 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, a 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 restarted; 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 nonoperational, 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 cause 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 the 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 is unable to communicate with the specified DPC in the SS7 network. Use these steps to determine if the issue is a communication problem between the Cisco BTS 10200 and the IP transfer point (ITP) or if it is related to communication problems between the ITP and the DPC:

Step 1 Use the Cisco BTS 10200 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 10-152. 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 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 10-157. Otherwise, proceed to Step 3.

Step 3 If you arrive at this step, there is probably communication between the Cisco BTS 10200 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. Please contact the Cisco TAC.

Step 5 Check whether the DPC has been removed from the Cisco BTS 10200 database. At the Cisco BTS 10200 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, that is, 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. No action is required.

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. The alarm is issued when service OOS message is received for ISDN trunks or 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 affected 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 the specified ISDN trunk group 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.

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.

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.

Call Agent Is Not Up or Is Not Responding to the Feature Server—Signaling (69)

The Call Agent Is Not Up or Is Not Responding to the Feature Server 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 Not Facility Associated Signaling—Signaling (78)

The Integrated Services Digital Network Single D-Channel Down for Not 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.

Trunking Gateway Unreachable—Signaling (79)

The Trunking Gateway Unreachable alarm (major) indicates that the trunking gateway is not responding to keep-alive Audit Endpoint messages. To correct the primary cause of the alarm, check the IP connectivity status between Cisco BTS 10200 call agent and the trunking gateway.

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. 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.

Note Heap memory usage is automatically monitored once per hour.

Insufficient Heap Memory—Signaling (81)

The Insufficient Heap Memory alarm (critical) indicates that there is insufficient heap memory. The primary cause of the alarm is that the H.323 signaling adapter was unable to allocate memory from the system. To correct the primary cause of the alarm, contact Cisco TAC for assistance.

Note Heap memory usage is automatically monitored once per hour.

Insufficient Shared Memory Pools—Signaling (82)

The Insufficient Shared Memory Pools alarm (critical) indicates that there is that there are not enough shared memory pools. The primary cause of the alarm is that the H.323 signaling adapter was unable to allocate storage. To correct the primary cause of the alarm, contact Cisco TAC for corrective action.

Error While Binding to Socket—Signaling (83)

The Error While Binding to Socket alarm (critical) indicates that an error occurred while the system was binding to the socket. To correct the primary cause of the alarm, contact Cisco TAC for corrective action.

Reached Maximum Socket Limit—Signaling (84)

The Reached Maximum Socket Limit alarm (critical) indicates that the Cisco BTS 10200 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 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 the Reason dataword for the failure cause and take action accordingly.

Remote H.323 Gateway Is Not Reachable—Signaling (86)

The Remote H.323 Gateway Is Not Reachable alarm (major) indicates that the remote H.323 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.

H.323 Message Parsing Error—Signaling (87)

The H.323 Message Parsing Error alarm (major) indicates that an H.323 message parsing error has occurred. The primary cause of the alarm is that the system was unable to successfully parse an incoming H.323 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.

H.323 Message Encoding Error—Signaling (88)

The H.323 Message Encoding Error alarm (major) indicates that an H.323 message encoding error has occurred. The primary cause of the alarm is that the system was unable to encode an H.323 message for sending. The alarm is indicative a software bug. To correct the primary cause of the alarm, contact Cisco TAC.

Gatekeeper not Available/Reachable—Signaling (89)

The Gatekeeper not Available/Reachable alarm (major) indicates that the gatekeeper is not available or the gatekeeper is not reachable. The primary cause of the alarm is that the gatekeeper is not available or is unreachable. To correct the primary cause of the alarm, check the network connectivity. Check to ensure the GK is reachable by trying to ping the GK IP address. If reachable, then check to ensure that the GK is configured up.

Alternate Gatekeeper Is Not Responding—Signaling (90)

The Alternate Gatekeeper Is Not Responding alarm (major) indicates that the alternate gatekeeper is not responding. The primary cause of the alarm is that the alternate gatekeeper is not responding. To correct the primary cause of the alarm, check network connectivity. Check to ensure the alternate GK is reachable by trying to ping the alternate GK IP address. If reachable, then check to ensure that the alternate GK is configured up.

Endpoint Security Violation—Signaling (91)

The Endpoint Security Violation alarm (major) indicates that an H.323 security violation has occurred. The primary cause of the alarm is that an H.323 security violation has occurred. To correct the primary cause of the alarm, check to make sure the password selections on the Cisco BTS 10200 and the gatekeeper are correct. The secondary cause of the alarm is that the H.323GW table may not be provisioned properly or there is a time synchronization problem between the Cisco BTS 10200 and/or the gatekeeper and the NTP server. To correct the secondary cause of the alarm, ensure that both the Cisco BTS 10200 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 or on the endpoint. To correct the primary cause of the alarm, contact Cisco TAC.

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 or on the endpoint. To correct the primary cause of the alarm, contact Cisco TAC.

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 or on the endpoint. To correct the primary cause of the alarm, contact Cisco TAC.

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.

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.

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.

H.323 Protocol Inconsistencies—Signaling (98)

The H.323 Protocol Inconsistencies alarm (minor) indicates that the H.323 endpoint and Cisco BTS 10200 are running different protocol versions. The primary cause of the alarm is that the H.323 endpoint and the Cisco BTS 10200 are running different protocol versions. This is only an issue where the endpoint is running a higher version of the H.323 protocol than the Cisco BTS 10200. To correct the primary cause of the alarm, contact Cisco TAC.

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.

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, reprovision 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.

H.323 Network Congested—Signaling (102)

The H.323 Network Congested alarm indicates (minor) that the H.323 application process has depleted its resources and no more calls can be completed. The primary cause of this alarm is that the H.323 application process has depleted its resources and no more calls can be completed. The high water mark has been reached and all new call requests are rejected until the low water mark is reached. To correct the primary cause of the alarm, reprovision the water marks or check the network for overload. Also verify that alternate routes have been provisioned on the Cisco BTS 10200.

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 Delivery Function Connection Down—Signaling (106)

The Enhanced Subscriber Authentication Cisco BTS 10200 Delivery Function Connection Down alarm (minor) indicates that the ESA Cisco BTS 10200 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. 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.

Simplex Only Operational Mode—Signaling (108)

The Simplex Only Operational Mode alarm (major) indicates that the Cisco BTS 10200 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 is configured as a simplex system.

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 is unable to communicate with an SGP at the SCTP protocol level. 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 CLI prompt:

```
status sctp-assoc id=<sctp-assoc-name>
```

If the response displays adminstrator 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/en/US/products/sw/wirelssw/ps1862/tsd_products_support_series_home.html

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. If the ASP on the active Cisco BTS 10200 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.

a. Determine the Cisco BTS 10200 configured values for the Cisco BTS 10200 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 are derived from the DNS name, which is given directly after the -h option. At the Cisco BTS 10200 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 configured local IP addresses are given in the Addresses: line.

b. Determine the ITP configured values of the ITP Cisco BTS 10200 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 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 side of the SCTP association. The two remote-IP addresses are the addresses that the ITP has configured for the Cisco BTS 10200 side of the SCTP association. Make sure all of these values match the values found in Step 2A.

c. Determine the Cisco BTS 10200 configured values for the ITP IP addresses and port.

On the Cisco BTS 10200 EMS CLI console, type the following:

```
CLI> show sctp-assoc id=<SCTP assoc id>
```

The output shows the IP addresses and port. For example:

```
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 IP addresses and port.

- Log on to the ITP and get into enable mode.
- Enter **sho run**.
- Press **Enter** until the m3ua (or sua) configuration is displayed. In our example, we are considering the SCTP association connection between the Cisco BTS 10200 and the ITP, so we will look at the ITP m3ua configuration. For example:

  ```
  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 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 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 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 is reachable from the ITP.

a. Log on to the ITP and get into enable mode.

b. Find the Cisco BTS 10200 SCTP association endpoint IP addresses by typing the following command:

show run

c. Press **Enter** until the ASP configuration is displayed. A section similar to the following will display the Cisco BTS 10200 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 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 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 shows either operator state -> SCTP-ASSOC out of service or operator state -> SCTP-ASSOC in service.

If the operator state still shows that the SCTP association is out-of-service, proceed to Step 7.

Step 7 Bounce the SCTP association from the ITP side by performing the following steps:

a. Log on to the ITP and get into enable mode.

b. Get into configure mode by typing configure terminal.

c. Type the following commands to bounce the SCTP association back in service:

```
va-2651-82(config)#cs7 asp hrn11asp
va-2651-82(config-cs7-asp)#shut
va-2651-82(config-cs7-asp)#no shut
va-2651-82(config-cs7-asp)#end
```

d. Determine if the SCTP association has come back in service by typing the following Cisco BTS 10200 CLI command:

```
status sctp-assoc id=<sctp-assoc-name>;
```

The output displays either operator state -> SCTP-ASSOC out of service or operator state -> SCTP-ASSOC in service.

If the operator 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 10-155 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 10-153, 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 an 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 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 10-153 to verify that your IP addresses and ports are properly configured on the Cisco BTS 10200.

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.

Signaling Gateway Failure—Signaling (113)

Note When a port on an ITP is removed from service by use of the **shut** command, multiple Signaling 113 and 114 alarms are raised (on status). When the port is recovered, through cycling of the ITP power, all alarms raised are cleared (off status) and are removed from CURRENT_ALARM table. However, not all cleared alarms (off status) are displayed on the subscriber terminal. Only the first instance of the cleared alarms (off status) with a variation in type, number, and component-ID **is** displayed. Multiple instances of the cleared alarms (off status) where the type, number, and component-ID are identical **are not** displayed.

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.

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 10-153 to determine why the associated SGPs are down.

Signaling Gateway Process Is Out of Service—Signaling (114)

Note When a port on an ITP is removed from service by use of the **shut** command, multiple Signaling 113 and 114 alarms are raised (on status). When the port is recovered, through cycling of the ITP power, all alarms raised are cleared (off status) and are removed from CURRENT_ALARM table. However, not all cleared alarms (off status) are displayed on the subscriber terminal. Only the first instance of the cleared alarms (off status) with a variation in type, number, and component-ID **is** displayed. Multiple instances of the cleared alarms (off status) where the type, number, and component-ID are identical **are not** displayed.

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 the 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 10-153. 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 a user part is unavailable on 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 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 10-153 to determine why the Cisco BTS 10200 is unable to communicate with any of the SGs at the M3UA layer. See the "Check the Stream Control Transmission Protocol Association Status" section on page 13-3 to determine why the Cisco BTS 10200 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 node that is trying to go into platform Active mode. It occurs when this Cisco BTS 10200 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. See the "Stream Control Transmission Protocol Association Degraded (One of Two Internet Protocol Connections Down)—Signaling (111)" section on page 10-153 to determine why the Cisco BTS 10200 is unable to communicate with any of the ITPs at the M3UA layer. Refer to the "Check the Stream Control Transmission Protocol Association Status" section on page 13-3 to determine why the Cisco BTS 10200 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. To correct the primary cause of the alarm, contact your service control point (SCP) service provider for assistance.

Note This alarm can occur when there is an SS7 outage affecting a nonadjacent remote destination point code (DPC) where the global title translation (GTT) database resides. The SS7 SCP subsystems in the Cisco BTS 10200 show the allowed status but the related DPC is shown to be unavailable.

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, reinitialize 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 points (SAPs) 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; such as, 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, reinitialize 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 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 the TSAP address of the remote entity is a domain name. Verify that 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 find out what is preventing the TSAP address from being reached. Verify that 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, eliminate 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.

Subscriber Line Faulty—Signaling (151)

The Subscriber Line Faulty alarm (minor) indicates that the residential gateway returned an error code in response to a command from the MGW. To correct the primary cause of the alarm, try controlling subscriber termination to OOS and back into INS using the Cisco BTS 10200 CLI command. If the problem persist after more calls, check the configuration in the Cisco BTS 10200 and the RGW. If the error codes returned by MGW are harmless, the error codes can be suppressed by adding a new entry in the MGCP-RETCODE-ACTION table and changing the EP-ACTION to reset/none.

Note The following additional troubleshooting information is applicable to Release 5.0 MR2 and above.

If the VXSM is OOS at the GW side, a 501 error message for CRCX/AUEP may be transmitted. This generally occurs if there is resource state mismatch between the Cisco BTS 10200 (ACTV IDLE) and the VXSM (DOWN). For additional information on the 501 error message, refer to Appendix A, "Recoverable and Nonrecoverable Error Codes."

When the mismatch occurs the default behavior is update for both the create connection (CRCX) and audit endpoint (AUEP) messages. For example:

```
CLI> add mgcp-retcode-action mgw-profile-id=<abc>; mgcp-msg=AUEP; mgcp-retcode=501;
call-action=release; ep-action=update

CLI> add mgcp-retcode-action mgw-profile-id=<abc>; mgcp-msg=AUEP; mgcp-retcode=501;
call-action=release; ep-action=update
```

If a 501 response is received for the CRCX message on execution of the EP-ACTION=update for CRCX, the Cisco BTS 10200 will start auditing the endpoint by sending an AuditEndpoint message requesting restart-method (rm parameter reported in the RSIP message, which indicates the service state at the GW). If the restart-method information reported in AUEP message is different from the Cisco BTS 10200 termination state, the termination state will be updated accordingly. If rm=forced, the termination oper-status is set to down; if rm=restart, the termination oper-status is set to up.

If a 501 response is received for the AUEP message on execution of the EP-ACTION=update for AUEP, the Cisco BTS 10200 will unconditionally mark the termination as down.

To clear down from the termination oper-status, you either need to control the trunk/subscriber-termination OOS/INS mode=forced; or trigger RSIP rm=restart from the GW.

Emergency Trunks Become Locally Blocked—Signaling (153)

The Emergency Trunks Become Locally Blocked alarm (critical) is issued when an emergency trunk (CAS, SS7, or ISDN) becomes locally blocked.

Emergency Trunks Become Remotely Blocked—Signaling (154)

The Emergency Trunks Become Remotely Blocked alarm (critical) is issued when an emergency trunk (CAS, SS7, or ISDN) becomes remotely blocked.

Integrated Services Digital Network Signaling Gateway Down—Signaling (156)

The Integrated Services Digital Network Signaling Gateway Down alarm (major) is issued when the Cisco BTS 10200 cannot communicate to the ISDN gateway. The primary cause of the alarm is that the Cisco BTS 10200 cannot communicate to the ISDN gateway due to a failure in the gateway. Additionally, the SCTP association might be down. To correct the primary cause of the alarm, find out whether the SCTP association is down and restore the SCTP association. The secondary cause of the alarm is that the IUA layer may be down in the gateway. If the IUA layer is down, it will be automatically recovered; no further action is required.

Integrated Services Digital Network Signaling Gateway Inactive—Signaling (157)

The Integrated Services Digital Network Signaling Gateway Inactive alarm (major) indicates that a **shutdown** command has been executed in the application server on the ISDN gateway side. No action needed. The application server will be automatically recovered.

Session Initiation Protocol Server Group Element Operationally Out of Service—Signaling (162)

The Session Initiation Protocol Server Group Element Operationally Out of Service alarm (critical) is issued when the Cisco BTS 10200 is unable to communicate with a remote SIP party. The primary cause of the alarm is that the Cisco BTS 10200 is unable to communicate with a remote SIP party (call-agent or proxy) over a SIP server group element. To correct the primary cause of the alarm, verify 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 TSAP address from the Event Report. If the same alarm is reported for other TSAP addresses on several softswitch trunk groups and/or server-group elements, then verify that the network connection is operational. The secondary cause of the alarm is that the remote SIP party is not operational. To correct the secondary cause of the alarm, diagnose the issue that prevents the TSAP address from being reached if a ping is not successful. Verify that the SIP application is running on the remote host and listening on the port specified in the TSAP address.

Routing Key Inactive—Signaling (163)

The Routing Key Inactive alarm (major) indicates that inactive acknowledgement messages were received from a Signaling Gateway. The SG or SCTP associations are probably down. To troubleshoot and correct the primary cause of the Routing Key Inactive alarm, investigate other alarms to see if SGs are down or the SCTP associations are down. Take corrective action according to those alarms. Also check the AS status for the routing context on ITP.

Signaling Gateway Traffic Mode Mismatch—Signaling (164)

The Signaling Gateway Traffic Mode Mismatch alarm (major) indicates that the traffic mode does not match on the Cisco BTS 10200 and the Signaling Gateway. To troubleshoot and correct the primary cause of the Signaling Gateway Traffic Mode Mismatch alarm, verify the AS traffic-mode configuration in the Signaling Gateway. Check that the SG internal redundancy mode for the traffic-mode setting has been set correctly in the Cisco BTS 10200.

Residential Gateway Endpoints Are Out of Service at the Gateway—Signaling (170)

The Residential Gateway Endpoints Are Out of Service at the Gateway alarm (minor) indicates that the residential gateway has been administratively taken OOS using the command at the gateway. To troubleshoot and correct the primary cause of the Residential Gateway Endpoints are out of Service at the Gateway alarm, bring the residential gateway administratively into INS using the command at the gateway.

Residential Gateway Unreachable—Signaling (171)

The Residential Gateway Unreachable alarm (minor) indicates that a MGCP signaling interop error has occurred with the residential media gateway. To troubleshoot and correct the primary cause of the Residential Gateway Unreachable alarm, check the IP connectivity status between the Cisco BTS 10200 call agent and the trunking gateway if the residential gateway is not physically connected, but controlled INS at the Cisco BTS 10200.

Multimedia Terminal Adapter Effective-Aggr-Id Becomes Unavailable Due to Its IP Address—Signaling (172)

The Multimedia Terminal Adapter Effective-Aggr-Id Becomes Unavailable Due to Its IP Address alarm (major) indicates that the MTA has been moved to new subnet which is not provisioned, or provisioned with the aggr-id=null. To troubleshoot and correct the primary cause of the Multimedia Terminal Adapter Effective-Aggr-Id Becomes Unavailable Due to Its IP Address alarm, provision the subnet aggr-id for the MTA.

ENUM Server Domain Cannot be Resolved Into Any IP Address —Signaling (173)

The ENUM Server Domain Cannot be Resolved Into Any IP Address alarm (critical) indicates that a misconfiguration has occurred in the DNS configuration. To troubleshoot and correct the cause of the alarm, fix the DNS configuration according the documentation.

ENUM Server Unavailable—Signaling (174)

The ENUM Server Unavailable alarm (critical) indicates that a network or server problem has occurred. To troubleshoot and correct the cause of the alarm, fix the network or server problem.

ENUM Server Farm Unavailable—Signaling (175)

The ENUM Server Farm Unavailable alarm (critical) indicates that a network or server problem has occurred. To troubleshoot and correct the cause of the alarm, fix the network or server problem.

No Resources Available to Launch ENUM Query—Signaling (176)

The No Resources Available to Launch ENUM Query alarm (critical) indicates that no resources are available to launch the ENUM query. The primary cause of the alarm is that there is internal or network congestion or that the server response is slow. To troubleshoot and correct the primary cause of the alarm, fix the network congestion or improve the server response.

Trunk Group Registration Expired—Signaling (179)

The Trunk Group Registration Expired alarm (major) indicates that a trunk group registration has expired. The primary cause of the alarm is that the trunk group did not register in time before the contact expiry. To troubleshoot and correct the primary cause of the Trunk Group Registration Expired alarm, verify that the receipt of a subsequent registration clears the alarm.

Transient Issue Occurred on the Emergency End-points—Signaling (182)

The Transient Issue Occurred on the Emergency End-points alarm (major) indicates that a transient error has occurred. The primary cause of the alarm is that:

- A transient error such as, 5XX error for CRCX, or a transient shm error, or an out-of-sequence message received at the MGA (MGCP protocol adapter) occurred on emergency end-points. Previously, the Signaling (152) alarm was raised at INFO level for all type of end-points. Beginning Release 6.0.3, the Signaling (182) is raised at a major severity level for such events on emergency end-points.
- Additionally, an error occurred for 911 call at BCM (Basic Call Module) like trunk group OOS, causing the Signaling (182) alarm to be raised at major severity, apart from other CALLP alarms at INFO level.

This behavior is controlled by a new CA_CONFIG type—SPECIAL-ALARM-FOR-911-TRANS-ISSUES DATATYPE. The default value of this field is N. Set it to Y to enable logging of Signaling (182).

To troubleshoot and correct the primary cause of the Transient Issue Occurred on the Emergency End-points alarm, take action based on the description provided when the alarm is logged. For example, if the description indicates that the trunk is OOS, control the trunk back to INS, if required. Since these alarms only denote a transient error and do not have any corresponding trigger point to clear the alarm, the operator needs to clear the alarms from the CLI frequently (if the operator has opted for logging of this alarm).

CHAPTER 11

Statistics Troubleshooting

Revised: August 10, 2011, OL-25016-01

Introduction

This chapter provides the information needed for monitoring and troubleshooting 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 for monitoring and correcting the statistics events
- Troubleshooting Statistics Alarms—Provides the information needed for troubleshooting and correcting the statistics alarms

Statistics Events and Alarms

This section provides a brief overview of all of the statistics events and alarms for the Cisco BTS 10200 Softswitch; the event and alarms are arranged in numerical order. Table 11-1 lists all of the statistics events and alarms by severity.

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

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	Information	Not Used
	Statistics (12)	Statistics (15)	Statistics (8)	Statistics (1)	
	Statistics (13)		Statistics (9)	Statistics (2)	
			Statistics (10)	Statistics (3)	
			Statistics (11)	Statistics (4)	
			Statistics (14)	Statistics (5)	
			Statistics (16)	Statistics (6)	
				Statistics (7)	

Statistics (1)

Table 11-2 lists the details of the Statistics (1) informational event. For additional information, refer to the "Test Report—Statistics (1)" section on page 11-15.

Table 11-2 Statistics (1) Details

Description	Test Report
Severity	Information
Threshold	10000
Throttle	0

Statistics (2)

Table 11-3 lists the details of the Statistics (2) informational event. For additional information, refer to the "Call Agent Measurement Collection Started—Statistics (2)" section on page 11-15.

Table 11-3 Statistics (2) Details

Description	Call Agent Measurement Collection Started
Severity	Information
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)

Table 11-3 lists the details of the Statistics (3) informational event. For additional information, refer to the "Call Agent Measurement Collection Finished—Statistics (3)" section on page 11-15.

Table 11-4 Statistics (3) Details

Description	Call Agent Measurement Collection Finished
Severity	Information
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)

Table 11-5 lists the details of the Statistics (4) informational event. 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 11-15.

Table 11-5 Statistics (4) Details

Description	Plain Old Telephone Service/Centrex/Telecommunications Data Link Monitor Feature Server Measurement Collection Started (POTS/CTX/TDM Feature Server Measurement Collection Started)
Severity	Information
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)

Table 11-6 lists the details of the Statistics (5) informational event. 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 11-15.

Table 11-6 Statistics (5) Details

Description	Plain Old Telephone Service/Centrex/Telecommunications Data Link Monitor Feature Server Measurement Collection Finished (POTS/CTX/TDM Feature Server Measurement Collection Finished)
Severity	Information
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)

Table 11-7 lists the details of the Statistics (6) informational event. For additional information, refer to the "Advanced Intelligent Network Feature Server Measurement Collection Started—Statistics (6)" section on page 11-15.

Table 11-7 Statistics (6) Details

Description	Advanced Intelligent Network Feature Server Measurement Collection Started (AIN Feature Server Measurement Collection Started)
Severity	Information
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)

Table 11-8 lists the details of the Statistics (7) informational event. For additional information, refer to the "Advanced Intelligent Network Feature Server Measurement Collection Finished—Statistics (7)" section on page 11-16.

Table 11-8 Statistics (7) Details

Description	Advanced Intelligent Network Feature Server Measurement Collection Finished (AIN Feature Server Measurement Collection Finished)
Severity	Information
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)

Table 11-9 lists the details of the Statistics (8) warning event. To monitor and correct the cause of the event, refer to the "Message Send Failure—Statistics (8)" section on page 11-16.

Table 11-9 Statistics (8) Details

Description	Message Send Failure
Severity	Warning
Threshold	100
Throttle	0
Datawords	Originating Process—STRING [40] Traffic Mgr Msg Type—STRING [40] Traffic Agent Msg Type—STRING [30]
Primary Cause	The 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	The hub is down.
Secondary Action	If the originating process is down, try to bring the process back into the normal state.
Ternary Cause	The 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).)

Statistics (9)

Table 11-10 lists the details of the Statistics (9) warning event. To monitor and correct the cause of the event, refer to the "Measurement Table Structured Query Language Read Error—Statistics (9)" section on page 11-16.

Table 11-10 Statistics (9) Details

Description	Measurement Table Structured Query Language Read Error (Measurement Table SQL Read Error)
Severity	Warning
Threshold	100
Throttle	0
Datawords	Measurement Table Na—STRING [40]
Primary Cause	There is no database connection or the connection is faulty.
Primary Action	Check to see if there are any other events generated that indicate there is a database problem.
Secondary Cause	The 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.

Statistics (10)

Table 11-11 lists the details of the Statistics (11) warning event. To monitor and correct the cause of the event, refer to the "Measurement Table Structured Query Language Write Error—Statistics (10)" section on page 11-17.

Table 11-11 Statistics (10) Details

Description	Measurement Table Structured Query Language Write Error (Measurement Table SQL Write Error)
Severity	Warning
Threshold	100
Throttle	0
Datawords	Measurement Table Na—STRING [40]
Primary Cause	There is no database connection or the connection is faulty.
Primary Action	Check to see if any other events are generated that indicate there is a database problem.
Secondary Cause	The 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.

Statistics (11)

Table 11-12 lists the details of the Statistics (11) warning event. To monitor and correct the cause of the event, refer to the "Measurement Collection Application Programming Interface Failure—Statistics (11)" section on page 11-17.

Table 11-12 Statistics (11) Details

Description	Measurement Collection Application Programming Interface Failure (Measurement Collection API 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 the 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	The 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	The 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 for the measurement period in which this event report was issued.

Statistics (12)

Table 11-13 lists the details of the Statistics (12) major alarm. To troubleshoot and correct the cause of the alarm, refer to the "Measurement Handshake Error—Schema Inconsistency—Statistics (12)" section on page 11-19.

Table 11-13 Statistics (12) Details

Description	Measurement Handshake Error—Schema Inconsistency
Severity	Major
Threshold	5
Throttle	0
Datawords	Schemas Out of Synchronization—STRING [64]
Primary Cause	Counters were added or deleted from the schema in Oracle but not in the call agent.
Primary Action	Add or delete the counters on the CA.
Secondary Cause	Load is installed incorrectly.
Secondary Action	Reinstall the load.

Statistics (13)

Table 11-14 lists the details of the Statistics (13) major alarm. 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 11-19.

Table 11-14 Statistics (13) Details

Description	Traffic and Measurements Module Application Programming Interface Failure (TMM API Failure)
Severity	Major
Threshold	1
Throttle	10
Datawords	TMM Error—FOUR_BYTES
Primary Cause	Unable to initialize shared memory.
Primary Action	Reconfigure and restart system.
Secondary Cause	Unable to attach to shared memory.
Secondary Action	Restart offending process.
Ternary Cause	Shared memory table overflow.
Ternary Action	Reconfigure/restart or fix problematic application.
Subsequent Cause	Shared memory exhaustion.
Subsequent Action	Reconfigure and restart system.

Statistics (14)

Table 11-15 lists the details of the Statistics (14) warning event. To monitor and correct the cause of the event, refer to the "MDII Trunk—Statistics (14)" section on page 11-18.

Table 11-15 Statistics (14) Details

Description	MDII Trunk
Severity	Warning
Threshold	100
Throttle	0
Datawords	Trunk Group—FOUR_BYTES CIC—FOUR_BYTES
Primary Cause	Calls on the MDII trunk termination are not being successfully completed.
Primary Action	The Cisco BTS 10200 system may take this trunk out of service if it does not take the full trunk group out of service.

Statistics (15)

Table 11-16 lists the details of the Statistics (15) minor alarm. To troubleshoot and correct the cause of the alarm, refer to the "Threshold Crossing Alert—Statistics (15)" section on page 11-19.

Table 11-16 Statistics (15) Details

Description	Threshold Crossing Alert
Severity	Minor
Threshold	100
Throttle	0
Datawords	Description—STRING [256]
Primary Cause	A threshold crossing has occurred.
Primary Action	Reduce the provisioning workload.

Statistics (16)

Table 11-17 lists the details of the Statistics (16) warning event. To monitor and correct the cause of the event, refer to the "Trunk Group Has Reached the MDII Alarm Threshold—Statistics (16)" section on page 18.

Table 11-17 Statistics (16) Details

Description	Trunk Group has Reached the MDII Alarm Threshold
Severity	Warning
Threshold	100
Throttle	0
Datawords	Trunk Group - FOUR_BYTES
Primary Cause	The trunk group has reached the MDII alarm threshold.
Primary Action	Check the performance status of trunk group.

Monitoring Statistics Events

This section provides the information you need for monitoring and correcting statistics events. Table 11-18 lists all of the statistics events in numerical order and provides cross-references to each subsection.

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

Table 11-18 Cisco BTS 10200 Statistics Events

Event Type	Event Name	Event Severity
Statistics (1)	Test Report—Statistics (1)	Information
Statistics (2)	Call Agent Measurement Collection Started—Statistics (2)	Information
Statistics (3)	Call Agent Measurement Collection Finished—Statistics (3)	Information
Statistics (4)	Plain Old Telephone Service/Centrex/Telecommunications Data Link Monitor Feature Server Measurement Collection Started—Statistics (4)	Information
Statistics (5)	Plain Old Telephone Service/Centrex/Telecommunications Data Link Monitor Feature Server Measurement Collection Finished—Statistics (5)	Information
Statistics (6)	Advanced Intelligent Network Feature Server Measurement Collection Started—Statistics (6)	Information
Statistics (7)	Advanced Intelligent Network Feature Server Measurement Collection Finished—Statistics (7)	Information
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
Statistics (14)	MDII Trunk—Statistics (14)	Warning
Statistics (15)	Threshold Crossing Alert—Statistics (15)	Minor
Statistics (16)	Trunk Group Has Reached the MDII Alarm Threshold—Statistics (16)	Warning

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, 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.

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.

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. If this warning event still occurs, contact Cisco TAC for technical support.

Measurement Collection Application Programming Interface Failure—Statistics (11)

The Measurement Collection Application Programming Interface Failure event serves as a warning that the measurement 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 measurements 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, and 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.

Note Traffic measurements will not be available for the affected call agent or feature server for 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 11-19.

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 11-19.

MDII Trunk—Statistics (14)

The MDII Trunk event serves as a warning that the calls on the MDII trunk termination are not being successfully completed. The Cisco BTS 10200 system might take the MDII trunk out of service if it does not take the full trunk group out of service.

Threshold Crossing Alert—Statistics (15)

The Threshold Crossing Alert alarm (minor) indicates that a threshold crossing has occurred. To troubleshoot and correct the cause of the Threshold Crossing Alert alarm, refer to the "Threshold Crossing Alert—Statistics (15)" section on page 11-19.

Trunk Group Has Reached the MDII Alarm Threshold—Statistics (16)

The Trunk Group Has Reached the MDII Alarm Threshold event serves as a warning that the trunk group has reached the MDII alarm threshold. To correct the cause of the event, check the performance status of the trunk group.

Troubleshooting Statistics Alarms

This section provides the information you need for monitoring and correcting statistics alarms. Table 11-19 lists all of the statistics alarms in numerical order and provides cross-references to each subsection.

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

Table 11-19 Cisco BTS 10200 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
Statistics (15)	Threshold Crossing Alert—Statistics (15)	Minor

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, reinstall 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 overflowed. 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.

Threshold Crossing Alert—Statistics (15)

The Threshold Crossing Alert alarm (minor) indicates that a threshold crossing has occurred. To correct the cause of the alarm, reduce the provisioning workload.

CHAPTER 12

System Troubleshooting

Revised: August 10, 2011, OL-25016-01

Introduction

This chapter provides the information needed for monitoring and troubleshooting 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 for monitoring and correcting the system events
- Troubleshooting System Alarms—Provides the information needed for troubleshooting and correcting the system alarms

System Events and Alarms

This section provides a brief overview of all of the system events and alarms for the Cisco BTS 10200 Softswitch; the event and alarms are arranged in numerical order. Table 12-1 lists all of the system events and alarms by severity.

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

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	Information	Not Used
System (13)	System (8)	System (2)	System (5)	System (1)	
	System (12)	System (3)	System (9)		
	System (15)	System (4)			
		System (6)			
		System (7)			
		System (10)			
		System (11)			
		System (14)			

System (1)

Table 12-2 lists the details of the System (1) information event. For additional information, refer to the "Test Report—System (1)" section on page 12-11.

Table 12-2 System (1) Details

Description	Test Report
Severity	Information
Threshold	100
Throttle	0
Primary Cause	This is a test report for the System category.
Primary Action	No action is required.

System (2)

Table 12-3 lists the details of the System (2) minor alarm. To troubleshoot and correct the cause of the alarm, refer to the "Inter-Process Communication Queue Read Failure—System (2)" section on page 12-15.

Table 12-3 System (2) Details

Description	Inter-Process Communication Queue Read Failure (IPC 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 the inter-process communication (IPC) process.
Primary Action	If the problem persists, contact Cisco TAC.

System (3)

Table 12-4 lists the details of the System (3) minor alarm. To troubleshoot and correct the cause of the alarm, refer to the "Inter-Process Communication Message Allocate Failure—System (3)" section on page 12-16.

Table 12-4 System (3) Details

Description	Inter-Process Communication Message Allocate Failure (IPC 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 the problem persists, contact Cisco TAC.

System (4)

Table 12-5 lists the details of the System (4) minor alarm. To troubleshoot and correct the cause of the alarm, refer to the "Inter-Process Communication Message Send Failure—System (4)" section on page 12-16.

Table 12-5 System (4) Details

Description	Inter-Process Communication Message Send Failure (IPC 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 that all components or processes are running. Attempt to restart any component or process that is not running.
Secondary Cause	An internal error has occurred.
Secondary Action	If the problem persists, contact Cisco TAC.

System (5)

Table 12-6 lists the details of the System (5) warning event. 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.

Table 12-6 System (5) Details

Description	Unexpected Inter-Process Communication Message Received (Unexpected IPC 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	Contact Cisco TAC.

System (6)

Table 12-7 lists the details of the System (6) minor alarm. To troubleshoot and correct the cause of the alarm, refer to the "Index List Insert Error—System (6)" section on page 12-16.

Table 12-7 System (6) Details

Description	Index List Insert Error (IDX 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 the problem persists, contact Cisco TAC.

System (7)

Table 12-8 lists the details of the System (7) minor alarm. To troubleshoot and correct the cause of the alarm, refer to the "Index List Remove Error—System (7)" section on page 12-16.

Table 12-8 System (7) Details

Description	Index List Remove Error (IDX 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 the problem persists, contact Cisco TAC.

System (8)

Table 12-9 lists the details of the System (8) major alarm. To troubleshoot and correct the cause of the alarm, refer to the "Thread Creation Failure—System (8)" section on page 12-16.

Table 12-9 System (8) Details

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, contact Cisco TAC.

System (9)

Table 12-10 lists the details of the System (9) warning event. To monitor and correct the cause of the event, refer to the "Timer Start Failure—System (9)" section on page 12-13.

Table 12-10 System (9) Details

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 the problem persists, contact Cisco TAC.

System (10)

Table 12-11 lists the details of the System (10) minor alarm. To troubleshoot and correct the cause of the alarm, refer to the "Index Update Registration Error—System (10)" section on page 12-17.

Table 12-11 System (10) Details

Description	Index Update Registration Error (IDX 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	Contact Cisco TAC.

System (11)

Table 12-12 lists the details of the System (11) minor alarm. To troubleshoot and correct the cause of the alarm, refer to the "Index Table Add Entry Error—System (11)" section on page 12-17.

Table 12-12 System (11) Details

Description	Index Table Add Entry Error (IDX 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 the problem persists, contact Cisco TAC.

System (12)

Table 12-13 lists the details of the System (12) major alarm. To troubleshoot and correct the cause of the alarm, refer to the "Software Error—System (12)" section on page 12-17.

Table 12-13 System (12) Details

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	The logic path is not handled by an algorithm in the code.
Primary Action	Save a trace log from around the time of the occurrence and contact Cisco TAC.

System (13)

Table 12-14 lists the details of the System (13) critical alarm. 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 12-17.

Table 12-14 System (13) Details

Description	Multiple Readers and Multiple Writers Maximum Q Depth Reached (MRMW Max Q 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 are flooding from a malfunctioning network element.
Primary Action	Check the messages to process.
Secondary Cause	Resource congestion or slow processing of messages from queue has occurred.
Secondary Action	Check the process and the system resources. You might need to fail over.

System (14)

Table 12-15 lists the details of the System (14) minor alarm. 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 12-17.

Table 12-15 System (14) Details

Description	Multiple Readers and Multiple Writers Queue Reached Low Queue Depth (MRMW 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	Messages are being received from the network at a high rate.
Primary Action	Check the messages to the system.
Secondary Cause	System or processing thread congestion has occurred.
Secondary Action	Check the process and the system resources.

System (15)

Table 12-16 lists the details of the System (15) major alarm. 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 12-18.

Table 12-16 System (15) Details

Description	Multiple Readers and Multiple Writers Throttle Queue Depth Reached (MRMW 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 are arriving at a rate much higher than the 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 slowdown in processing messages from queue has occurred.
Secondary Action	Check the platform CPU utilization, the IPC queue depth, and the overall availability of system resources.

Monitoring System Events

This section provides the information you need for monitoring and correcting system events. Table 12-17 lists all of the system events in numerical order and provides cross-references to each subsection.

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

Table 12-17 Cisco BTS 10200 System Events

Event Type	Event Name	Event Severity
System (1)	Test Report—System (1)	Information
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 12-15.

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 12-16.

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 12-16.

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.

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 12-16.

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 12-16.

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 12-16.

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.

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 12-17.

Index Table Add-Entry Error—System (11)

The Index Table Add-entry Error alarm (minor) indicates that an error occurred during the addition of 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 12-17.

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 12-17.

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 12-17.

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 12-17.

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 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 12-18.

Troubleshooting System Alarms

This section provides the information you need for monitoring and correcting system alarms. Table 12-18 lists all of the system alarms in numerical order and provides cross-references to each subsection.

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

Table 12-18 Cisco BTS 10200 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.

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. This alarm indicates a failure of IPC message allocation. It may be caused by following reasons:

- The message size is too big.
- No free entry in the message pool.
- Any internal errors.

To correct the primary causes of the alarm, contact Cisco TAC.

Prior to contacting Cisco TAC, collect statistics for the message pool and message queue.

To collect the statistics, use the **pdm.CAxxx** script in the /opt/OptiCall/CAxxx/bin directory.

Example:

```
pdm.CA146 -> 1.IPC Controls -> 2.Message Pool Stats & 6.MEssage Queue Stats
```

Also, use the **top** script to collect the current CPU usage.

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.

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.

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.

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.

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.

Index Table Add Entry Error—System (11)

The Index Table Add Entry Error alarm (minor) indicates that an error occurred during the addition of 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.

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 any 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.

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 slowdown in processing messages from the 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: August 10, 2011, OL-25016-01

Introduction

The chapter provides the information needed for conducting network troubleshooting on the Cisco BTS 10200 Softswitch. For Signaling System 7 (SS7) network troubleshooting information, refer to Chapter 10, "Signaling Troubleshooting." For additional troubleshooting information for specific protocols refer to the following protocol guides.

- *Cisco BTS 10200 Softswitch H.323 Guide, Release 6.0.3*
- *Cisco BTS 10200 Softswitch ISDN Guide, Release 6.0.3*
- *Cisco BTS 10200 Softswitch PacketCable Guide, Release 6.0.3*
- *Cisco BTS 10200 Softswitch SIP Guide, Release 6.0.3*
- *Cisco BTS 10200 Softswitch SS7 SIGTRAN Guide, Release 6.0.3*

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 Signaling Interface might lead to undesirable consequences or conditions.

Troubleshooting a Network Failure

Network failure issues can be caused by several problems. This section procedures you can use to isolate the cause of the problem. These procedures make up an iterative process, and they must be performed in the order indicated.

This section describes how to perform the following procedures:

Check 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 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. 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.

c. If the ASP on the active Cisco BTS 10200 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 "Find Out If the Application Service Provider Is Used by Any Application Server" section on page 13-6. Otherwise, continue to the next section.

Check 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. Enter **show sctp-assoc id-<sctp-assoc-name>** on the Cisco BTS 10200 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 are 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.

c. Repeat the "Check the Stream Control Transmission Protocol Association Status" section on page 13-3.

Step 5 Verify that the SCTP port on the Cisco BTS 10200 and the remote port of the ASP on the ITP are the same.

a. On the Cisco BTS 10200, open the platform.cfg file and locate the TCAP signaling adapter (TSA) section on the FSAIN/FSPTC(Feature Server for AIN services/Feature Server for POTS, Tandem, and Centrex) server, 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 SCTP port on the Cisco BTS 10200 and the remote port of the ASP on the ITP are the same, proceed to Step 6.

d. If the SCTP port on the Cisco BTS 10200 and the remote port of the ASP on the ITP are not the same, perform the following procedure:

- Correct the port setting on the ITP.
- Bounce the SCTP association on the Cisco BTS 10200.
- Repeat the"Check the Stream Control Transmission Protocol Association Status" section on page 13-3.

Step 6 Verify that the tsadns resolves to exactly the same remote-IP as the ASP on the ITP. If it does not, perform the following procedures as necessary:

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

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

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

d. Repeat the"Check the Stream Control Transmission Protocol Association Status" section on page 13-3.

Check the Internet Protocol Routing

Step 1 Ping the ITP addresses discovered in the "Check the Configuration" section on page 13-4 from the Cisco BTS 10200 in order to see if traffic is routed as planned.

Step 2 From the ITP, ping the Cisco BTS 10200 addresses discovered in the "Check the Configuration" section on page 13-4 to see if traffic is routed as planned.

Step 3 If routing is not as expected, correct the routing setup.

Step 4 Repeat the"Check the Stream Control Transmission Protocol Association Status" section on page 13-3.

Find Out 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 the ASP and continue.

Check the Internet Protocol Transfer Point T1 Card Provisioning

Enter **show controller t1 <slot/[bay/]port>** on the ITP. Verify that trunk level 1 (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
.....
```

Check the Internet Protocol Transfer Point Message Transfer Part 2 Serial Interface

To check for 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 is 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. Use this procedure:

- **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 shut down.

Step 3 After correcting the problem, continue to the next section.

Check the Internet Protocol Transfer Point-Signal Transfer Point Linkset Status

To check for problems with the ITP-signal transfer point (STP) linkset status, perform the following steps:

Step 1 Find out if 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.

Check the Internet Protocol Transfer Point Route

To check for problems with the ITP route, perform the following steps:

Step 1 Find out if there is a route to the destination point code provisioned in the Cisco BTS 10200 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 unavailable, the problem could be in the service provider's SS7 network. Contact the service provider to coordinate troubleshooting.

After this step is successfully passed, 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: August 10, 2011, OL-25016-01

Introduction

The chapter provides the general troubleshooting information you need for conducting 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 CORBA Adapter Interface Specification Programmer's Guide, Release 6.0.3*
- 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 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
- Call Agent Controlled Mode for RFC 2833 DTMF Relay Troubleshooting—Describes general troubleshooting procedures related to the call agent controlled mode for RFC 2833 DTMF relay
- NCS I10 and Audit Connection Troubleshooting—Describes the general troubleshooting procedures related to NCS I10 and the audit connection
- Multi-Lingual Support Troubleshooting—Describes the general troubleshooting procedures related to multi-lingual support
- Viewing Trace Logs for Throttled Flood of MGCP Messages From Specific Endpoint—Describes the general troubleshooting procedures related to viewing trace logs for a throttled flood of MGCP messages

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 Signaling Interface might lead to undesirable consequences or conditions.

Troubleshooting CORBA Problems

To troubleshoot CORBA interface problems, refer to the *Cisco BTS 10200 CORBA Adapter Interface Specification Programmer's Guide, Release 6.0.3*.

Troubleshooting Local Number Portability Problems

Problems can arise when a subscriber's telephone number is ported 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.

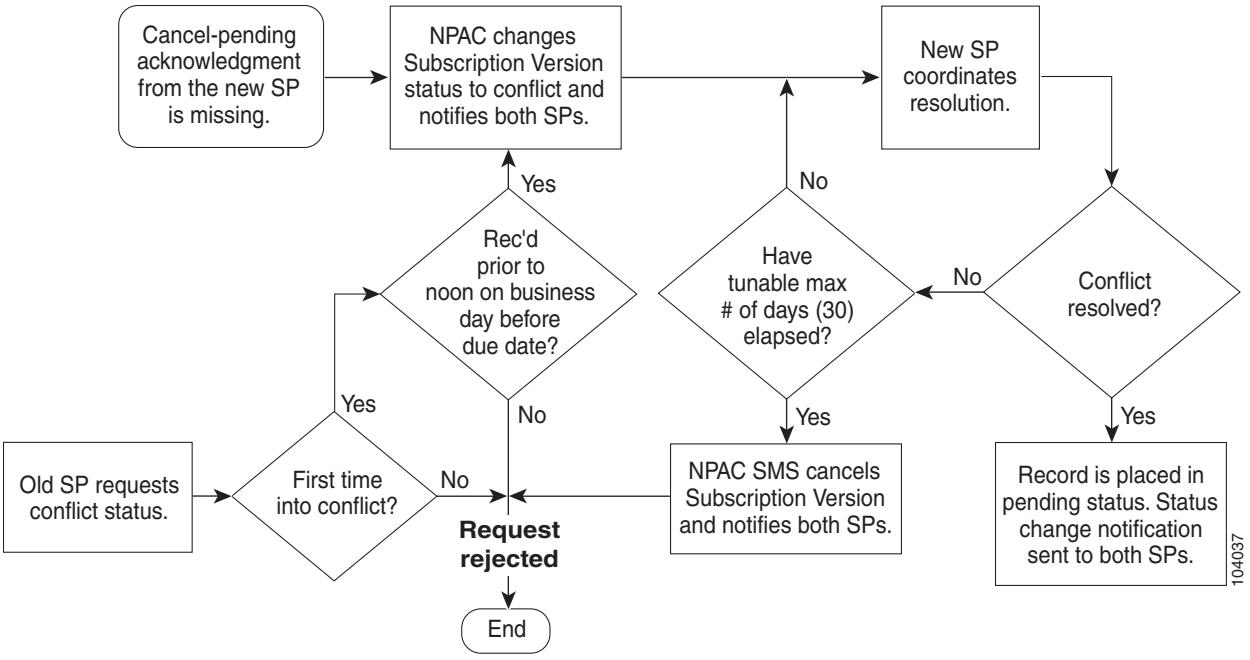
If either the old or new service provider did not send a notification to the NPAC SMS, the NPAC SMS notifies the service provider from which it did not receive a notification that it is expecting a notification. If the NPAC SMS receives the missing notification, and both notifications indicate agreement 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 might 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) address, 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 that one of the following three cases, as applicable:

- Verify that the ALERT_NOTIFY feature 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 the ALERT_NOTIFY feature is included in the default office service ID (if the feature is intended to be offered to all subscribers on the switch).

Note In the procedures included in this document, the alerting notification feature is provisioned using the feature identifier **FNAME=ALERT_NOTIFY**. The feature identifier can be any unique string of up to 16 ASCII characters chosen by the service provider. If you are not sure of the name used in your system for this feature, use the **show feature** command and view the system response to find the name.

Example:

```
SHOW FEATURE-SERVER;
SHOW FEATURE FNAME=ALERT_NOTIFY;
SHOW CA-CONFIG TYPE=DEFAULT-OFFICE-SERVICE-ID;
SHOW SERVICE ID=<the value of the default-office-service-id>
SHOW SERVICE ID=6543;
SHOW SUBSCRIBER-SERVICE-PROFILE SERVICE-ID=6543;
```

Step 4 If a TSAP address is used for the 3PTYFS, verify that the domain name is correctly provisioned in the DNS and resolves to the intended 3PTYFS.

Step 5 Enter the CLI command to check for Signaling Alarm 12—Feature Server Is Not Up or Is Not Responding to Call Agent. If this alarm is raised, there is a communications problem between the Cisco BTS 10200 and the 3PTYFS.

Example:

```
show alarm type=signaling;
show alarm type=signaling; number=12;
```

The following details apply to the Signaling (12) alarm:

- For a 3PTYFS that is more than one hop away from the Cisco BTS 10200, Signaling (12) alarm is raised when communications between the Cisco BTS 10200 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 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 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, SS7 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 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 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 protocol problems.

Troubleshooting H.323 Problems

To troubleshoot H.323 problems, refer to the *Cisco BTS 10200 Softswitch H.323 Guide, Release 6.0.3*.

Troubleshooting Integrated Services Digital Network Problems

To troubleshoot Integrated Services Digital Network (ISDN) problems, refer to the *Cisco BTS 10200 Softswitch ISDN Guide, Release 6.0.3*.

Troubleshooting PacketCable Problems

To troubleshoot PacketCable problems, refer to the *Cisco BTS 10200 Softswitch PacketCable Guide, Release 6.0.3*.

Troubleshooting SIP Problems

To troubleshoot SIP problems, refer to the *Cisco BTS 10200 Softswitch SIP Guide, Release 6.0.3*.

Troubleshooting SS7 SIGTRAN Problems

To troubleshoot Signaling System 7 SIGTRAN problems, refer to the *Cisco BTS 10200 Softswitch SS7 SIGTRAN Guide, Release 6.0.3*.

File Configuration—bts.properties

This section provides instructions for editing and configuring the bts.properties file. The default content of the /opt/ems/etc/bts.properties file is in listed in Table 14-1.

Note Modification of the bts.properties file should not be attempted without Cisco TAC support or supervision.

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

Parameter	Variable
reportDir=	/opt/ems/report
reportDirSize=	50000000
reportSuffix=	.html
logDefLevel=	Information
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
invalidChars=	‘‘’; # spaces or other white space characters are considered invalid.
LERGDuration=	86400000
throttleEnable=	N

Editing—bts.properties

Note Modification of the bts.properties file should not be attempted without Cisco TAC support or supervision.

Use the following instructions to edit the bts.properties file:

Step 1 Edit the /opt/ems/etc/bts.properties file to change the desired parameter(s).

Step 2 Shut down and restart the affected processes.

Edit Example—bts.properties

The following instructions show how to configure the bts.properties file to enable debugging.

Note Modification of the bts.properties file should not be attempted without Cisco TAC support or supervision.

Step 1 Open the /opt/ems/etc/bts.properties file.

Step 2 Set logDefLevel=debug.
//valid logging options are: info, debug, error, warning, fatal

Step 3 Start a new CLI session.
//su - btsuser

Step 4 Look for the log information in the /opt/ems/log/<username>.log. It is //btsuser.log in this case.

Privacy Screening Troubleshooting

This section lists several privacy screening troubleshooting symptoms and solutions.

Symptom 1

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

Solution 1

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 2

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

Solution 2

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

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

Symptom 3

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

Solution 3

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

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

Symptom 4

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

Solution 4

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 with which the subscriber is associated.

Call Agent Controlled Mode for RFC 2833 DTMF Relay Troubleshooting

This section describes general troubleshooting procedures related to the call agent controlled mode for RFC 2833 DTMF relay.

General Troubleshooting Procedures

This section explains how to troubleshoot the following conditions:

- Basic Call Cannot Be Established
- No DTMF Relay Involving H.323 Endpoints

Basic Call Cannot Be Established

Problem: A basic call cannot be established through the MGW.

Symptom: The CRCX message sent to the MGW results in failure.

Diagnosis: Determine whether the MGW supports CA-controlled RFC 2833 DTMF relay. (See the MGW vendor documentation for information on MGW features.)

Resolution: If the MGW does not support CA-controlled RFC 2833 DTMF relay, set dtmf-telephone-event-enabled=N in the QoS table associated with the endpoint.

No DTMF Relay Involving H.323 Endpoints

Problem: RFC 2833 DTMF relay does not work on the H.323 gateway or endpoint.

Symptom: DTMF tones do not go through.

Diagnosis: Determine whether the RFC 2833 payload configured on the H.323 gateway or endpoint matches the payload configured on the Cisco BTS 10200.

Resolution: Ensure that the value of rfc2833-payload in the applicable h323-tg-profile or h323-term-profile table is set to the same value as that on the H.323 gateway or endpoint.

NCS I10 and Audit Connection Troubleshooting

This section explains how to troubleshoot the following conditions:

General Troubleshooting Information

Call Agent (CA) log files are located in /opt/OptiCall/CA[XYZ]/bin/logs directory, where XYZ is the CA instance (for example CA146). If you need to call Cisco TAC regarding a call-processing issue, first collect the log files from this directory if possible.

Troubleshooting the Timeout Queue

Problem: Due to a change in NCS protocol specifications, MGCP command timeout has increased by a factor of 2.

Symptoms: Increased memory usage on slow networks and during major outages of MGCP devices.

Diagnosis: Memory usage returns to normal when network connectivity to MGCP devices is restored.

Resolution: Great care needs to be taken when MGCP-T-HIST and MGCP-T-MAX parameters are provisioned in the ca-config table. If necessary, reduce the values of MGCP-T-HIST and/or MGCP-T-MAX parameters. Note that MGCP-T-HIST must be greater than or equal to MGCP-T-MAX + 10 seconds; otherwise the provisioned settings are ignored by the system (the system reverts to the default values for these parameters).

Note For a detailed discussion of keepalive timeout parameters, see Appendix B, "System Usage of MGW Keepalive Parameters, Release 6.0."

Troubleshooting QoS

Problem: Endpoint does not support silence suppression and/or echo cancellation.

Symptom: Silence suppression and/or echo cancellation parameters provisioned on the Cisco BTS 10200 are not reflected in MGCP device behavior.

Diagnosis:

1. Through CLI commands, take the MGCP device out of service. Make sure to take the entire MGCP device out of service (control mgw...) because disabling the terminations is not sufficient.
2. Put the MGCP device back in service.

Use network packet analysis software to observe the response to an AUEP command. Look through each "A:" (capabilities) line and verify that "s:on" (silence suppression supported) and/or "e:on" (echo cancellation supported) are not present.

Resolution:

- If the endpoint reports “e:on” in its capabilities, but provisioned echo cancellation settings are ignored, verify that EC-SUPP is enabled for the MGCP device in the mgw-profile table.
- Upgrade the MGCP device firmware.
- Contact the device manufacturer if the MGCP device advertises support for silence suppression/echo cancellation but does not report it to the CA.

Troubleshooting Audit Connection

Problem: Stray connections have not been removed after failover.

Symptoms: Endpoint(s) unable to place feature calls, dropped active calls after a Cisco BTS 10200 failover.

Diagnosis: Place a call through the endpoint. Use network packet analysis software to observe any negative CreateConnection (CRCX) ACK responses from the MGCP device. Check whether error messages in the negative ACK responses indicate that connection resources are not available (which suggests that the resources are not being cleaned up).

Resolution: Enable AuditConnection support for MGCP profile corresponding to MGCP device.

Multi-Lingual Support Troubleshooting

This section describes general troubleshooting procedures.

Ensure the subscriber has MLS using report billing_record:

```
DIALEDDIGITS=*56
CALLTERMINATIONCAUSE=NORMAL_CALL_CLEARING
```

*56 is the VSC entered by the subscriber to start MLS. NORMAL_CALL_CLEARING shows the IVR successfully completed its service.

If NORMAL_CALL_CLEARING does not return, check both the service and subscriber_service_profile tables:

```
btsadmin> show service id=mlstest
ID=mlstest
FNAME1=MLS
btsadmin>show subscriber_service_profile sub-id=2212437211
SUB_ID=2212437211
SERVICE_ID=mlstest
```

If you hear a reorder-tone from a SIP phone, ensure the status of the Cisco BTS 10200 announcement table is all of the following:

```
btsadmin> status tt tgn-id=889;cic=all
889 1   ADMIN_INS     TERM_ACTIVE_IDLE      ACTV   IDLE   NON_FAULTY
```

If you hear a click from an MGCP phone, ensure the status of the Cisco BTS 10200 announcement table is all of the following:

```
btsadmin> status tt tgn-id=889;cic=all
889 1   ADMIN_INS     TERM_ACTIVE_IDLE      ACTV   IDLE   NON_FAULTY
```

If you hear a reorder tone instead of audio, ensure the release_cause table routes to correct MS:

```
btsadmin> show release_cause
ID=1
ANNC_ID=18
btsadmin> show announcement
...
ANNOUNCEMENT_FILE=ann_id_18.au
ROUTE_GUIDE_ID=10013
```

Ensure that the IVR script points to the correct MS and that the MLS has an FNAME:

```
btsadmin> show ivr_script_profile
FNAME=MLS
IVR_ACCESS_MODE=IVR
IVR_ROUTE_GUIDE_ID=10013
IVR_SCRIPT_PKG_TYPE=BAU
```

Ensure that the annc-tg-profile table is correct:

```
ANNC_LANG_FORMAT_SUPPORTED=N for IPUnity
ANNC_LANG_FORMAT_SUPPORTED=Y for Cognitronics
```

Turn on trace in the Cisco BTS 10200 Call Agent (CA) for MLS, set MGCP on the CA to info5 level, and examine the BAU code from the MS:

```
TC_11.3.1_CA.log:..           MGA    00-00.           |<<<< RECV FROM: 10.1.31.2
FROM-PORT=2427 TO-PORT=2727 <<<<|
TC_11.3.1_CA.log-..           MGA    00-00.           |ntfy 717
annc/1@sj-ms1-s4.sjc-devtest.com MGCP 1.0 NCS 1.0^M|
TC_11.3.1_CA.log-..           MGA    00-00.           |X: 2B00000007^M|
TC_11.3.1_CA.log-..           MGA    00-00.           |O: A/of(rc=601)^M|
TC_11.3.1_CA.log-..           MGA    00-00.           ||snd_rcv.c:260
```

Error: Need

Explanation: The mls-annc-mult-factor token value is lower than the number of announcements existing on the MS.

Recommended Action: Provision the mls-annc-mult-factor token value greater than the number of announcements on the MS.

Error: Return Code 601: File not found

Explanation: MSs are limited to 40-character filenames. These 40 characters include the extension (typically a wav) and the announcement-file-prefix: for example fra_, eng_ and spa_.

Recommended Action: Change the filename length to less than 40 characters.

Viewing Trace Logs for Throttled Flood of MGCP Messages From Specific Endpoint

The Cisco BTS 10200 can detect an incoming flood of messages from an individual MGCP-based MGW or endpoint. When such a flood occurs, the Cisco BTS 10200 automatically throttles messages coming from that specific resource. If the flood condition stops, the system releases the throttle. The system also deletes wild-carded messages (for example, RSIP <tid> *@mgw.net) received from any MGW. This detection and throttling mechanism is not customer configurable.

The system displays one of the following traces in logs at the INFO3 level:

- Message dumped for termIdx=<term id> due to high incoming message rate.
- Message dumped for mgIdx=<mg id> due to high incoming message rate.

Note Log info levels are listed in the "Logs" section on page C-15 in Appendix C, "Overload Control."

Platform Core File Alarm

The Cisco BTS 10200 core file monitor feature provides Cisco BTS 10200 customers with an alarm notification whenever a core file is generated on a Cisco BTS 10200 platform system. The Cisco BTS 10200 core file monitor feature also removes core files automatically when disk space is critically low or when the core file has aged beyond a maximum allowable time.

Core files are generated and stored in the bin directory for the binary executable which generated the core. The normal procedure to be followed by the operator is to move the core files as they are generated to another storage area. The monitoring of core files with alarm notification will remind the system operator to perform this process.

The Cisco BTS 10200 core file monitor enhancement is driven by the problem that core files are huge (2–4 GB) and eventually cause a disk full condition resulting in a switchover. In the field, operators rely on a process crash alarm to alert them that a core file is present. The core file monitor alarm provides an additional periodic reminder that operator action must be taken to move core files from the system.

Note See the *Cisco BTS 10200 Softswitch Network and Subscriber Feature Descriptions, Release 6.0.3* guide for a complete list of subscriber features supported by the Cisco BTS 10200.

Planning

This section provides information on prerequisites and limitations applicable to the Cisco BTS 10200 core file monitor feature:

- Prerequisites—Tasks or conditions (outside the immediate scope of this document) that are required before these new Cisco BTS 10200 features can work as specified
- Restrictions and limitations for this feature—Special conditions or scenarios for which these features might not work, or might behave in an unexpected manner

Prerequisites

The Cisco BTS 10200 must be upgraded to Release 5.0 and above for the Cisco BTS 10200 core file monitor feature to be active.

Restrictions and Limitations

The Cisco BTS 10200 must be upgraded to Release 5.0 and above for the Cisco BTS 10200 core file monitor feature to be active.

Configuring

The configuration of the Cisco BTS 10200 core file monitor feature is dependent upon the settings in the cfm.cfg file. Table 14-2 lists the parameters and conditions within the cfm.cfg file for configuring the Cisco BTS 10200 core file monitor feature.

Table 14-2 Core File Monitor Configuration File Parameters and Conditions

Parameter	Condition
CORE_FILE_MONITOR_DISABLE	If set to true, the core file monitor audit is not performed. Default setting is false.
CORE_FILE_ALARM_ENABLE	If set to false, the core file monitor alarm is not issued when a core file is found in the network element bin directory. Default setting is true.
CORE_FILE_MINIMUM_SPACE	This is the minimum free file space in megabytes which will trigger the automatic deletion of the oldest core files. Default is 5 GB.
CORE_FILE_AGE_TO_DELETE	This is the maximum time in hours that a core file can exist before it is automatically deleted. Default is 72 hours.
CORE_FILE_AGE_DELETE_ENABLE	If set to true, core files are deleted automatically when their maximum age is reached. Default is true.
CORE_FILE_SPACE_DELETE_ENABLE	If set to true, the oldest core files are deleted when free file space is low. Default is true.

For details on troubleshooting the "Core File Present" condition, refer to Core File Present—Audit (25), page 2-20.

CHAPTER 15

Diagnostic Tests

Revised: August 10, 2011, OL-25016-01

Introduction

This chapter describes diagnostic tests that can be performed on media gateways, subscriber terminations, and trunk terminations. All media gateways and subscriber and trunk terminations must be in the maintenance state for testing. The following tests are described in this chapter:

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 might 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 maintenance state.

Step 1 Force the media gateway into maintenance 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 maintenance state.

Step 1 Force the subscriber termination into maintenance state:

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

Step 2 Display the Test Menu.

```
diag subscriber-termination;
```

Reply Example:

```
Reply: Diagnostic Subscriber Menu.
===
(1) Subscriber MGCP Connectivity Test
(2) Subscriber Termination Connection Test
(3) Subscriber Termination Ring Test
(4) ALL
```

Note Test 1 tests if MGCP has access to the termination.

Test 2 tests if there is a path to the device (ping).

Test 3 tests if the subscriber can be rung. The Ring parameter must be specified in seconds for this test. The default is 5 seconds.

Test 4 performs tests 1 through 3.

Step 3 To perform a specific test, use the following examples as a guide.

```
diag subscriber-termination id=sub2-ctx2; test=1;
```

Reply Example:

```
SUBSCRIBER LINE DIAGNOSTIC TEST EXECUTED -> diag subscriber-termination
ID -> sub2-ctx2
TEST-TYPE -> ADM-MGW-MGCP-CONNECTIVITY-TEST
TEST-DURATION -> 10
RESULT -> TEST-SUCCESS
REASON -> PASSED: Reason: AUEP-NACK received with RespCode = 510
Reply: Diagnostic command executed.
```

```
diag subscriber-termination id=sub-ubr3-1@cisco.com; test=2;
```

Reply Example:

```
SUBSCRIBER LINE DIAGNOSTIC TEST EXECUTED -> diag subscriber-termination
ID -> sub-ubr3-1@Cisco.com
TEST-TYPE -> ADM-TERM-CONNECTION-TEST
TEST-DURATION -> 55
RESULT -> TEST-SUCCESS
REASON -> PASS successfully.
Reply: Diagnostic command executed.
```

```
diag subscriber-termination id=sub-ubr3-1@cisco.com; test=3; ring-duration=10;
```

Reply Example:

```
SUBSCRIBER LINE DIAGNOSTIC TEST EXECUTED -> diag subscriber-termination
ID -> sub-ubr3-1@Cisco.com
TEST-TYPE -> ADM-TERM-RING-TEST
TEST-DURATION -> 9989
RESULT -> TEST-SUCCESS
REASON -> PASSED
Reply: Diagnostic command executed.
```

Step 4 Force the subscriber termination into INS state:

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

Note Ring-duration values are 0–999 (Default = 5). Maximum ring time is 30 seconds regardless of whether the duration is set higher than or equal to 31.

Signaling System 7 Trunk Termination Tests

This section describes the tests that can be performed on Signaling System 7 (SS7) trunk terminations. All terminations must be in the maintenance state for testing.

Step 1 Force the SS7 trunk termination into maintenance 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
Test 2: SS7 Termination Connection Test
Test 3: SS7 COT Test
Test 4: SS7 CQM Test
Test 5: SS7 CVT Test
Test 6: SS7 CIC Audit
Test 0: ALL Tests
```

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 0 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 maintenance state for testing.

Step 1 Force the ISDN trunk termination into maintenance state:

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

Step 2 Display the Test Menu.

```
diag isdn-trunk-termination
```

Reply Example:

```
Reply: Diagnostic ISDN Trunk Group Menu.
===
(1) ISDN MGCP Connectivity Test
(2) ISDN Termination Connection Test
(3) ALL
```

Note Test 1 tests if MGCP has access to the ISDN termination.

Test 2 tests if there is a path to the device (ping).

Test 3 performs tests 1 and 2.

Step 3 To perform a specific test, use the following examples as a guide:

```
diag isdn-trunk-termination test=1; tgn-id=17; cic=1;
```

Reply Example:

```
TRUNK DIAGNOSTIC TEST EXECUTED -> diag trunk
TG-NUM -> 17
CIC -> 1
TEST-TYPE -> ADM-MGW-MGCP-CONNECTIVITY-TEST
TEST-DURATION -> 0
RESULT -> TEST-SUCCESS
REASON -> PASSED: Reason: AUEP-NACK received with RespCode = 510
Reply: Diagnostic command executed.
```

```
diag isdn-trunk-termination test=2; tgn-id=17; cic=1;
```

Reply Example:

```
TRUNK DIAGNOSTIC TEST EXECUTED -> diag trunk
TG-NUM -> 17
CIC -> 1
TEST-TYPE -> ADM-TERM-CONNECTION-TEST
TEST-DURATION -> 0
RESULT -> TEST-SUCCESS
REASON -> PASSED: Reason: AUEP-NACK received with RespCode = 510
Reply: Diagnostic command executed.
```

Step 4 Force the ISDN trunk termination into MAINT state:

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

Channel-Associated Signaling Trunk Termination Tests

This section describes the tests that can be performed on channel-associated signaling (CAS) trunk terminations. All terminations must be in the maintenance state for testing.

Step 1 Force the CAS trunk termination into maintenance 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 maintenance state for testing.

Step 1 Force the Announcement trunk termination into maintenance 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 call agent itself in a production network. It can cause performance degradation.

Snoop can be used on the Cisco BTS 10200 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 set up 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. There are probably multiple roots, so 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 **snoop** 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 example, interfaces qfe0 and qfe4 must be snooped.

Step 2 Issue the **snoop** command. The syntax might differ 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 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 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 like those 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.

```
# 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. 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 uses to communicate 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. 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 uses to communicate 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 Registration, Admissions, 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. 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) in the following way:

```
# 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

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 number called from the signal switching point (SSP).
- Query Tool E800VER Command—Send a database query to the SCP as if it were 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

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;
```

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 15-19.

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 one in 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 subsystem, enter the following command:

```
CLI> query toll-free-msg-type; opc-id=opc;
MESSAGE-TYPE=AIN01
Reply: Success:
CLI>
```

Parameter Boundary Error

The query can fail if you enter invalid data for a specific parameter. In the following example, a value outside the boundary of expected values for the trigger-criteria parameter has been specified:

```
CLI> query toll-free; called-dn=8002550002; calling-dn=2182640018; lata=100;
trigger-criteria=12; opc-id=opc;
Invalid parameter value.
trigger_criteria=12; Enter one of the following values: [3,6,7,8,9,10].
CLI>
```

To resolve this error, enter a valid value for the specified parameter.

Record Does Not Exist

In the following example, a value has been entered for a lata that has not been provisioned:

```
CLI> query toll-free; called-dn=8002550002; calling-dn=2182640018; lata=101;
trigger-criteria=9; opc-id=opc;
Reply: Failure: LATA 101 does not exist
CLI>
```

To resolve this error, enter a provisioned local access and transport area (LATA).

Local Network Failure

When communication is lost between the Cisco BTS 10200 and the IP transfer point (ITP) gateway, a local network failure might 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 title translation (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 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

Table 15-3 identifies the measurements generated by the POTS Feature Server for the QVT feature.

Table 15-3 QVT POTS Tool 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

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;
```

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_PIC1=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; EL_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-prof; STATUS=INS; DIRECTION=BOTH; SEL_POLICY=ASC; GLARE=EVEN;
ALT_ROUTE_ON_CONG=N; SIGNAL_PORTED_NUMBER=N; POP_ID=1; REMOTE_SWITCH_LRN=2122129999;
DIAL_PLAN_ID=dp19; Description=TG to BTS12; DEL_DIGITS=0; OPER_STATUS=NF;
TRAFFIC_TYPE=TANDEM; ANI_BASED_ROUTING=N; CLLI=DAL177DS3;
CALL_CTRL_ROUTE_ID=bts12-ccroute1; MGCP_PKG_TYPE=T; ANI_SCREENING=N; SEND_RDN_AS_CPN=N;

Reply: Success:

CLI>
```

Translation Verification Tool Measurements

Table 15-4 identifies the measurements generated by the TVT Tool.

Table 15-4 TVT Tool Counters

Counter Label	Counter Description
TOOLS_LNP_QUERY_ATTMP	The total number of times the reporting feature server received a request to perform an LNP query from the QVT tool
TOOLS_LNP_QUERY_SUCC	The total number of times the reporting feature server received a request to perform an LNP query from the QVT tool and completed it successfully
TOOLS_TOLLFREE_QUERY_ATTMP	The total number of times the reporting feature server received a request to perform a toll free query from the QVT tool
TOOLS_TOLLFREE_QUERY_SUCC	The total number of times the reporting feature server received a request to perform a toll free query from the QVT tool and completed it successfully

Using Query Verification Tool and Translation Verification Tool Together

It may be necessary to use both QVT and TVT queries to diagnose routing of a call. If the results of a **translate** command indicate that a toll-free or LNP query is generated, execute the QVT query. Use the results of the QVT query to generate another TVT query.

The following example illustrates verifying routing of a call from (972) 233-1286 to (800) 255-3002:

Step 1 Execute a **TVT translate** command:

```
CLI> translate line calling-dn=9722331286; called-dn=8002553002;

TRANSLATE LINE ON CALL AGENT CA146 IS...->
TABLEINFO ->
******TOLL FREE CALL NEEDS AN 800 QUERY******

Reply: Success:

CLI>
```

Step 2 The **translate** command indicates that a Toll-Free query is required. Perform the QVT query to do the number translation.

```
CLI> query toll-free called-dn=8002553002; calling-dn=9722331286; lata=100; opc-id=opc;

TOLL FREE QUERY ON FEATURE SERVER FSAIN520 IS...->
RESULT->
OPC=7-2-1
SSN=254
TT-254
SCP-Point-Code=1-101-0
Message-Type=IN/1
Called Number=8002553002
Translated Number=7034323002
Carrier=0000

Reply: Success:

CLI>
```

Step 3 The translated number returned by the QVT query can now be used in a TVT **translate** command to verify call routing.

```
CLI> translate line calling-dn=9722331286; called-dn=7034323002;

TRANSLATE LINE ON CALL AGENT CA146 IS... ->

TABLEINFO ->

TABLE: SUBSCRIBER

ID=sub_1_6; CATEGORY=INDIVIDUAL; NAME=sub16; STATUS=ACTIVE; ADDRESS1=1651 n glenville
suite 200; ADDRESS2=Richardson tx 75081; BILLING_DN=9722331286; DN1=9722331286;
PRIVACY=NONE; RING_TYPE_DN1=1; TERM_ID=aaln/S1/6; MGW_ID=c2421_1; PIC1=NONE; PIC2=NONE;
PIC3=NONE; GRP=N; USAGE_SENS=Y; SUB_PROFILE_ID=sub_pmlhg_prof1; 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;
INTRA_STATE=Y; GAP_ROUTING=N; CLDPTY_CTRL_REL_ALWD=N;

TABLE: ROUTE_GUIDE

ID=ssp1-rg; POLICY_TYPE=ROUTE; POLICY_ID=ssp1-route;

TABLE: ROUTE

ID=ssp1-route; TGN1_ID=3; DEL_DIGITS1=0; DEL_DIGITS2=0; DEL_DIGITS3=0; DEL_DIGITS4=0;
DEL_DIGITS5=0; DEL_DIGITS6=0; DEL_DIGITS7=0; DEL_DIGITS8=0; DEL_DIGITS9=0; DEL_DIGITS10=0;
TG_SELECTION=RR;

TABLE: TRUNK_GRP

ID=3; CALL_AGENT_ID=CA146; TG_TYPE=SS7; NUM_OF_TRUNKS=24; DPC=1-12-1;
TG_PROFILE_ID=ssp1-tg-prof; STATUS=INS; DIRECTION=BOTH; SEL_POLICY=ASC; GLARE=EVEN;
ALT_ROUTE_ON_CONG=N; SIGNAL_PORTED_NUMBER=N; POP_ID=1; REMOTE_SWITCH_LRN=2122129999;
DIAL_PLAN_ID=dp19; Description=TG to BTS12; DEL_DIGITS=0; OPER_STATUS=NF;
TRAFFIC_TYPE=TANDEM; ANI_BASED_ROUTING=N; CLLI=DAL177DS3;
CALL_CTRL_ROUTE_ID=bts12-ccroute1; MGCP_PKG_TYPE=T; ANI_SCREENING=N; SEND_RDN_AS_CPN=N;

Reply: Success:

CLI>
```

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_PROFILE_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_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=AUTO; ACCESS_TYPE=COMBINED;
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_DIGITS4=0;
DEL_DIGITS5=0; DEL_DIGITS6=0; DEL_DIGITS7=0; DEL_DIGITS8=0; DEL_DIGITS9=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_PROFILE_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;
STATUS_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=COMBINED;
POI=INTER_ENDOFFICE; PERFORM_LNP_QUERY=N;



Reply: Success:
```

Example 2

In this example, a subscriber dials a 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;
SEND_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; 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 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;
SEND_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_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;
STATUS_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=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;
SEND_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=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=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;
SEND_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_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;
STATUS_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=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;
SEND_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_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;
STATUS_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=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 Cisco BTS 10200 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_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_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=AUTO; 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; OVERDECADIC_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_WITH_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_DIGITS=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_REL_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_ID=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=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=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 tests on any line side PacketCable Network-based Call Signaling protocol specification/Media Gateway Control Protocol (NCS/MGCP) Residential Gateways. The network loopback tests can be initiated from designated test endpoints. This section also describes enhancements to the TDM bearer path test call feature.

This section contains the following:

Overview

The Network Loopback Test for NCS/MGCP Endpoints feature provides a testing device with the capability to perform network loopback tests from any line side NCS/MGCP residential gateways or media termination adapters (MTAs). These loopback tests are initiated from designated test endpoints (subscribers) controlled by the Cisco BTS 10200.

The basic network loopback test feature is service affecting. In other words, while a network loopback call is in progress, the endpoint is considered busy.

The Cisco BTS 10200 network loopback and network continuity tests also have a service-not-affected mode. In this mode, the Cisco BTS 10200 will attempt to create coexisting test connections on the test device; however, if the endpoint does not have enough resources, the Cisco BTS 10200 gives preference to regular calls, processing them first before it processes any test calls.

In the service-affected mode the Cisco BTS 10200 will not try to initiate other calls, even if the MTA/TGW can set up multiple connections (PARALLEL-TEST-CONN-SUPP=Y).

The Cisco 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 Cisco 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 Cisco 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 shows the steps required to configure the originating line (media gateway profile) to identify a network loopback call.

Note These tasks include examples of CLI commands that illustrate how to provision the specific feature. Most of these tables have additional tokens that are not included in the examples. For a complete list of all CLI tables and tokens, see the Cisco BTS 10200 Softswitch CLI Database.

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

The following procedure is a dedicated NLB testing device configuration example. Change TEST-LINE-TYPE to different values (other than NTE) to change test origination type.

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

The following procedure is 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

The following procedure is 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

The following procedure is 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 call-subtype-profile.

```
add call-subtype-profile call-type=TEST_CALL; call-subtype=NONE; qos-id=1;
```

Step 3 Add dial-plan-profile.

```
add dial-plan-profile id=test; nanp-dial-plan=N
```

Step 4 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

The following procedure is 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;
```

Network Loopback Test for Network-Based Call Signaling/Media Gateway Control Protocol Endpoints

This section describes network loopback testing for network-based call signaling and media gateway control protocol endpoints feature and includes descriptions of the following:

- 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 BTS 10200 allows NCS/MGCP endpoints in a trunk group to be provisioned as a dedicated test trunk group.

The provisioning of the test trunk group determines if incoming calls arriving on the dedicated test trunk groups trigger the Cisco BTS 10200 to complete the test call through a Network Loopback (NLB) or Network Continuity Test (NCT). The category of the test call is preprovisioned on the dedicated test trunk groups—all calls from a particular test trunk group invoke the same test category while calls from another test trunk group might invoke a different test category. A test call from a test device utilizes the eMTA directory number (DN) the same as any other regular dialed digit string.

The called party number format is:

<Test-data>

Where:

<Test-data> = DN (for example, the NCS/MGCP dialed digits signaled to the Cisco BTS 10200 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 Cisco BTS 10200 allows a shared test trunk group, where the category of the test to be run is specified by the test-prefix. Cisco 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 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, the Cisco BTS 10200 Softswitch will perform the longest match) of the test prefix and its length, whether it is 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 call subtype profile.

Step 6 Configure the main subscriber ID for testing trunk-grp.

Step 7 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 can arise, for example, when a subscriber complains about not being able to receive calls. The first item to check would be the registration status; use the **sip-reg-contact** command. The next item would be to check for events regarding authentication failures and so on.

The following examples show the usage of the **sip-reg-contact** command. The first example shows an expired contact and the second example shows a registered contact or current contact.

Example 1:

Use 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:

Use 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.

Use the following example shows you how to run a SHR:

```
CLI> report system-health period=720;
```

Period	The length of time to collect 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 of the Cisco BTS 10200, an **SHR** command is scheduled to execute at midnight every 24 hours.

To schedule multiple **SHR** command(s) at different times, you can use the **command scheduler add** command 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 involve running two commands, bts_audit and bts_sync. The bts_audit and bts_sync tools are designed to improve speed and integrity of auditing and syncing the Cisco BTS 10200 databases. 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 fast audit and sync tools feature consists of two UNIX 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. The database mismatches are synchronized using the bts_sync tool.

The bts_audit tool determines the table sizes 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 checksums

are compared, and if they are not equal, the network element data file is transferred to the EMS. On the EMS, the data is compared row by row, and mismatches are printed to a file that can be used by the bts_sync tool to restore synchronization of the table on the network element.

Restrictions and Limitations

The Cisco BTS 10200 fast audit and sync tools feature 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 an 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 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 mismatches 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 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 lines.
- 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 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 of the test prefix and its length. We recommend a pattern of 1 to 6 digits—but the first digit cannot be "1", the Cisco BTS 10200 performs the longest match.
- <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 the call type subprofile.

Step 4 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. Take the following steps to change the service affect of the test.

Step 1 Execute the following commands to change service affect for either NCT or NLB testing. The default service affect 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 and 9.

Sample Configurations

The following sample configurations illustrate how to configure the Cisco BTS 10200 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 CLI Database.

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 sample steps for the NTE NLB trunk test over an ISDN trunk feature.

	Perform the Following Command or Action:	Purpose and Comments
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 call-subtype-profile** call-type=TEST_CALL; call-subtype=NONE; qos-id=1;	Provision the Call Subtype Profile table.
Step 3	**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 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 4	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.
Step 5	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 sample steps for the NTE NLB line test over an ISDN trunk with "service affecting" turned on feature.

	Perform the Following Command or Action:	Purpose and Comments
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 call-subtype-profile** call-type=TEST_CALL; call-subtype=NONE; qos-id=1;	Provision the Call Subtype Profile table.
Step 3	**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 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 4	**add ca-config** type=nlb-test-service-affecting=y; datatype=boolean; value=y;	Provision the Call Agent Configuration table with service affecting on.
Step 5	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.
Step 6	Take the subscriber under test off-hook.	There is no dial tone.
Step 7	Call the subscriber under test from another subscriber.	Call is treated, and the test call is still active.
Step 8	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 sample steps for the NTE NLB line test over an ISDN trunk with "service affecting" turned off feature.

	Perform the Following Command or Action:	Purpose and Comments
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 call-subtype-profile** call-type=TEST_CALL; call-subtype=NONE; qos-id=1;	Provision the Call Subtype Profile table.
Step 3	**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 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 4	**add ca-config** type=nlb-test-service-affecting=n; datatype=boolean; value=n;	Provision the Call Agent Configuration table with service affecting off.
Step 5	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.
Step 6	Take the subscriber under test off-hook.	There is a dial tone.

	Perform the Following Command or Action:	Purpose and Comments
Step 7	Call the subscriber under test from another subscriber.	Call is set up, and the test call is released.
Step 8	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 sample steps for the NTE NLB line test over an ISDN trunk with "service affecting" turned on and parallel test connection support turned on feature. The call is from the subscriber under test.

	Perform the Following Command or Action:	Purpose and Comments
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 call-subtype-profile** call-type=TEST_CALL; call-subtype=NONE; qos-id=1;	Provision the Call Subtype Profile table.
Step 3	**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 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 4	**add ca-config** type=nlb-test-service-affecting=n; datatype=boolean; value=n;	Provision the Call Agent Configuration table with service affecting off.
Step 5	**change mgw-profile** id=isdnNLB; parallel-test-conn-supp=y;	Turn on support parallel test connection in the Media Gateway Profile table.
Step 6	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.
Step 7	Take the subscriber under test off-hook.	There is a dial tone.
Step 8	Call the subscriber under test from another subscriber.	Call is set up, and the test call is still active.
Step 9	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 sample steps for the NTE NLB line test over an ISDN trunk with "service affecting" turned off and parallel test connection support turned on feature. The call is to the subscriber under test.

	Perform the Following Command or Action:	Purpose and Comments
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 call-subtype-profile** call-type=TEST_CALL; call-subtype=NONE; qos-id=1;	Provision the Call Subtype Profile table.

	Perform the Following Command or Action:	Purpose and Comments
Step 3	**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 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 4	**add ca-config** type=nlb-test-service-affecting=n; datatype=boolean; value=n;	Provision the Call Agent Configuration table with service affecting off.
Step 5	**change mgw-profile** id=isdnNLB; parallel-test-conn-supp=y;	Turn on support parallel test connection in the Media Gateway Profile table.
Step 6	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.
Step 7	Take the subscriber under test off-hook.	There is a dial tone.
Step 8	Call the subscriber under test from another subscriber.	Call is set up, and the test call stays up.
Step 9	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 sample steps for the NTE NLB trunk test over an ISDN trunk feature.

	Perform the Following Command or Action:	Purpose and Comments
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 call-subtype-profile** call-type=TEST_CALL; call-subtype=NONE; qos-id=1;	Provision the Call Subtype Profile table.
Step 3	**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 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 4	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.
Step 5	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 sample steps for NTE NCT line test over an ISDN trunk with "service affecting" turned on feature.

	Perform the Following Command or Action:	Purpose and Comments
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 call-subtype-profile** call-type=TEST_CALL; call-subtype=NONE; qos-id=1;	Provision the Call Subtype Profile table.
Step 3	**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 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 4	**add ca-config** type=nlb-test-service-affecting=y; datatype=boolean; value=y;	Provision the Call Agent Configuration table with service affecting on.
Step 5	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.
Step 6	Take the subscriber under test off-hook.	There is no dial tone.
Step 7	Call the subscriber under test from another subscriber.	Call is treated, and the test call is still active.
Step 8	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 sample steps for the NTE NCT line test over an ISDN trunk with "service affecting" turned off feature.

	Perform the Following Command or Action:	Purpose and Comments
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 call-subtype-profile** call-type=TEST_CALL; call-subtype=NONE; qos-id=1;	Provision the Call Subtype Profile table.
Step 3	**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 4	**add ca-config** type=nlb-test-service-affecting=n; datatype=boolean; value=n;	Provision the Call Agent Configuration table with service affecting off.
Step 5	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.
Step 6	Take the subscriber under test off-hook.	There is a dial tone.

	Perform the Following Command or Action:	Purpose and Comments
Step 7	Call the subscriber under test from another subscriber.	Call is set up, and the test call is released.
Step 8	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 sample steps for the NTE NCT line test over an ISDN trunk with service "affecting turned" on and parallel test connection support turned on feature. The call is from the subscriber under test.

	Perform the Following Command or Action:	Purpose and Comments
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 call-subtype-profile** call-type=TEST_CALL; call-subtype=NONE; qos-id=1;	Provision the Call Subtype Profile table.
Step 3	**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 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 4	**add ca-config** type=nlb-test-service-affecting=n; datatype=boolean; value=n;	Provision the Call Agent Configuration table with service affecting off.
Step 5	**change mgw-profile** id=isdnNLB; parallel-test-conn-supp=y;	Turn on support parallel test connection in the Media Gateway Profile table.
Step 6	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.
Step 7	Take the subscriber under test off-hook.	There is a dial tone.
Step 8	Call the subscriber under test from another subscriber.	Call is set up, and the test call is still active.
Step 9	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 sample steps for the NTE NCT line test over an ISDN trunk with "service affecting" turned off and parallel test connection support turned on feature. The call is to the subscriber under test.

	Perform the Following Command or Action:	Purpose and Comments
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 call-subtype-profile** call-type=TEST_CALL; call-subtype=NONE; qos-id=1;	Provision the Call Subtype Profile table.

	Perform the Following Command or Action:	Purpose and Comments
Step 3	**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 4	**add ca-config** type=nlb-test-service-affecting=n; datatype=boolean; value=n;	Provision the Call Agent Configuration table with service affecting off.
Step 5	**change mgw-profile** id=isdnNLB; parallel-test-conn-supp=y;	Turn on support parallel test connection in the Media Gateway Profile table.
Step 6	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.
Step 7	Take the subscriber under test off-hook.	There is a dial tone.
Step 8	Call the subscriber under test from another subscriber.	Call is set up, and the test call stays up.
Step 9	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 sample steps for the NTE NLB trunk test over an ISDN trunk feature.

	Perform the Following Command or Action:	Purpose and Comments
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 call-subtype-profile** call-type=TEST_CALL; call-subtype=NONE; qos-id=1;	Provision the Call Subtype Profile table.
Step 3	**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 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.

	Perform the Following Command or Action:	Purpose and Comments
Step 4	From the test equipment, dial the NTE NLB trunk test call (553+trunk digits+members).	—
Step 5	Hang up the test call and verify the Billing call type.	—

NCT Trunk Loopback Test Over an ISDN Trunk

This section provides sample steps for the NTE NLB trunk test over an ISDN trunk feature.

	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 call-subtype-profile** call-type=TEST_CALL; call-subtype=NONE; qos-id=1;	Provision the Call Subtype Profile table.
Step 3	**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 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 4	**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.
Step 5	From the test equipment, dial the NTE NLB trunk test call (554+trunk digits+members) (trunk).	—
Step 6	Hang up the test call and verify the Billing call type.	—

Enhanced Traffic Measurement

The Cisco BTS 10200 supports traditional PSTN measurements as well as additional requirements demanded by the IP and ATM backbones over which the services are offered. 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 is 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 Cisco 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
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

Table 15-5 Event Reports Supported by Measurement Subsystem (continued)

Type and Number	Severity	Description	Meaning
Statistics (11)	Warning	Measurement Collection API Failure	Issued whenever the traffic agent process in any of the Cisco BTS 10200 elements is unable to access the counter stored within shared memory by means of 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
Statistics (14)	Warning	MDII Trunk	Calls on the MDII trunk termination are not being successfully completed
Statistics (15)	Minor	Threshold Crossing Alert	A threshold crossing has occurred

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 CLI Database and the *Cisco BTS 10200 Operations and Maintenance Guide, Release 6.0.3*.

Provisioning Measurement Report Types

The Cisco 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 25 types of measurement data generated by the Cisco BTS 10200 (see the following list):

- 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 Cisco 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 characters 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 preprovisioned 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 0 minutes after the hour for consistency. This is an optional token that is preprovisioned 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 for querying summary reports of measurement data from the database on the Element Management System (EMS). This mechanism provides the ability for specifying 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, 2007 and place the data into CSV files for FTP.

Note Any measurement counters that do not contain data for a given interval are kept out of the generated reports. Only counters that were pegged are presented in the resulting summaries.

```
report measurement-isdn-summary start-time=2007-03-27 10:00:00; end-time=2007-03-27
12:00:00; call-agent-id=CA146; output=isdn-report; output-type=csv;
```

```
report measurement-callp-summary start-time=2007-03-27 10:00:00; end-time=2007-03-27
12:00:00; call-agent-id= CA146; output=callp-report; output-type=csv;

report measurement-mgcp-summary start-time=2007-03-27 10:00:00; end-time=2007-03-27
12:00:00; call-agent-id= CA146; output=mgcp-report; output-type=csv;

report measurement-sim-summary start-time=2007-03-27 10:00:00; end-time=2007-03-27
12:00:00; call-agent-id= CA146; output=sim-report; output-type=csv;

report measurement-pots-local-summary start-time=2007-03-27 10:00:00; end-time=2007-03-27
12:00:00; feature-server-id=PCT01; output=pots-local-report; output-type=csv;

report measurement-pots-misc-summary start-time=2007-03-27 10:00:00; end-time=2007-03-27
12:00:00; feature-server-id=PCT01; output=pots-misc-report; output-type=csv;

report measurement-pots-sle-summary start-time=2007-03-27 10:00:00; end-time=2007-03-27
12:00:00; feature-server-id=PCT01; output=pots-sle-report; output-type=csv;

report measurement-pots-acar-summary start-time=2007-03-27 10:00:00; end-time=2007-03-27
12:00:00; feature-server-id=PCT01; output=pots-acar-report; output-type=csv;

report measurement-pots-cos-summary start-time=2007-03-27 10:00:00; end-time=2007-03-27
12:00:00; feature-server-id=PCT01; output=pots-cos-report; output-type=csv;

report measurement-pots-cot-summary start-time=2007-03-27 10:00:00; end-time=2007-03-27
12:00:00; feature-server-id=PCT01; output=pots-cot-report; output-type=csv;

report measurement-ainsvc-summary start-time=2007-03-27 10:00:00; end-time=2007-03-27
12:00:00; feature-server-id=AIN01; output=ainsvc-report; output-type=csv;

report measurement-sccp-summary start-time=2007-03-27 10:00:00; end-time=2007-03-27
12:00:00; feature-server-id=AIN01; output=sccp-report; output-type=csv;

report measurement-tcap-summary start-time=2007-03-27 10:00:00; end-time=2007-03-27
12:00:00; feature-server-id=AIN01; output=tcap-report; output-type=csv;

report measurement-m3ua-summary start-time=2007-03-27 10:00:00; end-time=2007-03-27
12:00:00; sgp-id=sg-001; output=m3ua-report; output-type=csv;

report measurement-sua-summary start-time=2007-03-27 10:00:00; end-time=2007-03-27
12:00:00; sgp-id=sg-001; output=sua-report; output-type=csv;

report measurement-sctp-summary start-time=2007-03-27 10:00:00; end-time=2007-03-27
12:00:00; sctp-assoc-id=assoc-001; output=sctp-report; output-type=csv;

report measurement-isup-summary start-time=2007-03-27 10:00:00; end-time=2007-03-27
12:00:00; tgn-id=dallas01; output=isup-report; output-type=csv;

report measurement-audit-summary start-time=2007-03-27 10:00:00; end-time=2007-03-27
12:00:00; call-agent-id=CA146; output=audit-report; output-type=csv;

report measurement-sia-summary start-time=2007-03-27 10:00:00; end-time=2007-03-27
12:00:00; call-agent-id=CA146; output=sia-report; output-type=csv;

report measurement-billing-summary start-time=2007-03-27 10:00:00; end-time=2007-03-27
12:00:00; call-agent-id=CA146; output=billing-report; output-type=csv;

report measurement-em-summary start-time=2007-03-27 10:00:00; end-time=2007-03-27
12:00:00; call-agent-id=CA146; output=em-report; output-type=csv;

report measurement-dqos-summary start-time=2007-03-27 10:00:00; end-time=2007-03-27
12:00:00; aggr-id=AGGR01; output=dqos-report; output-type=csv;
```

```
report measurement-snmp-summary start-time=2007-03-27 10:00:00; end-time=2007-03-27
12:00:00; output=snmp-report; output-type=csv;

report measurement-tg-usage-summary start-time=2007-03-27 10:00:00; end-time=2007-03-27
12:00:00; tgn-id=dallas01; call-agent-id=CA146; output=tg-report; output-type=csv;

report measurement-tg-usage-summary start-time=2007-03-27 10:00:00; end-time=2007-03-27
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=2007-03-27 10:00:00; end-time=2007-03-27
12:00:00; call-agent-id=CA146; output=anm-report; output-type=csv;

report measurement-h323-summary start-time=2007-03-27 10:00:00; end-time=2007-03-27
12:00:00; call-agent-id=CA146; output=h323-report; output-type=csv;

report measurement-call-tools-summary start-time=2007-03-27 10:00:00; end-time=2007-03-27
12:00:00; call-agent-id=CA146; output=call-tools-report; output-type=csv;

report measurement-ain-tools-summary start-time=2007-03-27 10:00:00; end-time=2007-03-27
12:00:00; feature-server-id=AIN01; output=ain-tools-report; output-type=csv;

report measurement-pct-tools-summary start-time=2007-03-27 10:00:00; end-time=2007-03-27
12:00:00; feature-server-id=PCT01; output=pct-tools-report; output-type=csv;
```

Command Line Tokens

Table 15-6 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 time for the search. 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 time for the search. This is an optional token. When omitted, it results in the display of the last collected interval.
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.

Table 15-6 Command Line Tokens Associated with Measurement Report Summaries (continued)

Command Line Token	Description
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 prepended 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 applicable only to the following measurement types: • call-tools • billing • callp • mgcp • isdn • audit • sia • sim • anm • h323 • tg-usage • em
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 applicable only to the following measurement types: • pct-tools • ain-tools • ainsvc • sccp • tcap • pots-local • pots-misc • pots-sle • pots-acar • pots-cos • pots-cot

Table 15-6 Command Line Tokens Associated with Measurement Report Summaries (continued)

Command Line Token	Description
tgn-id	The trunk group numbers used to report measurement data. This is an optional token that is applicable only 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 applicable only 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 applicable only to the following measurement type: • sctp
aggr-id	The aggregation ID for reporting measurement data. This is an optional token that is applicable only to the following measurement type: • dqos

Reporting Current Interval Counts

The Cisco BTS 10200 system provides a CLI command for querying in-progress partial interval counts of measurement data from the actual source of the data. This mechanism provides the ability for specifying 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 for generating reports on the various types of measurements currently being collected from call agents and feature servers on March 27th, 2007, 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;
```

Table 15-7 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 start time for the interval during which a search is made through 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 prepended 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) format 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 applicable only 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 applicable only 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 currently stored on the disk (all). If this token is used on the command line, it overrides 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 for specifying 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.

In the following examples, all of the currently accumulating counters in call agents and feature servers are cleared:

```
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;
```

Table 15-8 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 applicable only 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 applicable only 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 Cisco BTS 10200 through the command line or FTP interfaces.

ISDN Protocol Counters

Table 15-9 identifies the ISDN protocol counters.

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 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 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.
ISDN_INFORMATION_TX	The number of ISDN information messages sent from the reporting call agent.

Table 15-9 ISDN Protocol Counters (continued)

Counter Label	Counter Context
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 applicable only to ETSI PRI.
ISDN_SUSPEND_RX	The number of ISDN suspend messages received by the reporting call agent. **Note** This counter is applicable only to ETSI PRI.
ISDN_SUSPEND_ACK_TX	The number of ISDN suspend ACK messages sent from the reporting call agent. **Note** This counter is applicable only to ETSI PRI.
ISDN_SUSPEND_ACK_RX	The number of ISDN suspend ACK messages received by the reporting call agent. **Note** This counter is applicable only to ETSI PRI.
ISDN_SUSPEND_REJ_TX	The number of ISDN suspend reject messages sent from the reporting call agent. **Note** This counter is applicable only to ETSI PRI.
ISDN_SUSPEND_REJ_RX	The number of ISDN suspend reject messages received by the reporting call agent. **Note** This counter is applicable only to ETSI PRI.
ISDN_RESUME_TX	The number of ISDN resume messages sent from the reporting call agent. **Note** This counter is applicable only to ETSI PRI.
ISDN_RESUME_RX	The number of ISDN resume messages received by the reporting call agent. **Note** This counter is applicable only to ETSI PRI.
ISDN_RESUME_ACK_TX	The number of ISDN resume ACK messages sent from the reporting call agent. **Note** This counter is applicable only to ETSI PRI.
ISDN_RESUME_ACK_RX	The number of ISDN resume ACK messages received by the reporting call agent. **Note** This counter is applicable only to ETSI PRI.
ISDN_RESUME_REJ_TX	The number of ISDN resume reject messages sent from the reporting call agent. **Note** This counter is applicable only to ETSI PRI.

Table 15-9 ISDN Protocol Counters (continued)

Counter Label	Counter Context
ISDN_RESUME_REJ_RX	The number of ISDN resume reject messages received by the reporting call agent. **Note** This counter is applicable only to ETSI PRI.
ISDN_USER_INFO_TX	The number of ISDN user information messages sent from the reporting call agent. **Note** This counter is applicable only to ETSI PRI.
ISDN_USER_INFO_RX	The number of ISDN user information messages received by the reporting call agent. **Note** This counter is applicable only to ETSI PRI.
ISDN_CONG_CNTL_TX	The number of ISDN congestion control messages sent from the reporting call agent. **Note** This counter is applicable only to ETSI PRI.
ISDN_CONG_CNTL_RX	The number of ISDN congestion control messages received by the reporting call agent. **Note** This counter is applicable only to ETSI PRI.
ISDN_SEGMENT_TX	The number of ISDN segment messages sent from the reporting call agent. **Note** This counter is applicable only to ETSI PRI.
ISDN_SEGMENT_RX	The number of ISDN segment messages received by the reporting call agent. **Note** This counter is applicable only 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.
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.

Table 15-10 Call Processing Counters (continued)

Counter Label	Counter Context
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.
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.

Table 15-10 Call Processing Counters (continued)

Counter Label	Counter Context
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.
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.

Table 15-10 Call Processing Counters (continued)

Counter Label	Counter Context
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 a CAS originator to an SS7 terminator on the reporting call agent.
CALLP_CAS_ISDN_CALL	The number of successfully completed calls from a CAS originator to an ISDN terminator on the reporting call agent.
CALLP_CAS_SIP_CALL	The number of successfully completed calls from a CAS originator to an SIP terminator on the reporting call agent.
CALLP_CAS_MGCP_CALL	The number of successfully completed calls from a CAS originator to an MGCP terminator on the reporting call agent.
CALLP_CAS_CAS_CALL	The number of successfully completed calls from a CAS originator to a 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.
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.

Table 15-10 Call Processing Counters (continued)

Counter Label	Counter Context
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 H.323 call attempts on the reporting call agent.
CALLP_H323_TERM_ATTMP	The number of terminating H.323 call attempts on the reporting call agent.
CALLP_H323_ORIG_FAIL	The number of originating H.323 call attempts that failed on the reporting call agent.
CALLP_H323_TERM_FAIL	The number of terminating H.323 call attempts that failed on the reporting call agent.
CALLP_H323_CALL_SUCC	The number of originating and terminating H.323 call attempts that completed successfully on the reporting call agent.
CALLP_H323_CALL_ABAND	The number of terminating and originating H.323 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 H.323 terminator on the reporting call agent.
CALLP_SS7_H323_CALL	The total number of successfully completed calls from an SS7 originator to an H.323 terminator on the reporting call agent.
CALLP_SIP_H323_CALL	The total number of successfully completed calls from a SIP originator to an H.323 terminator on the reporting call agent.
CALLP_MGCP_H323_CALL	The total number of successfully completed calls from an MGCP originator to an H.323 terminator on the reporting call agent.
CALLP_CAS_H323_CALL	The total number of successfully completed calls from a CAS originator to an H.323 terminator on the reporting call agent.
CALLP_H323_SIP_CALL	The total number of successfully completed calls from an H.323 originator to a SIP terminator on the reporting call agent.
CALLP_H323_ISDN_CALL	The total number of successfully completed calls from an H.323 originator to an ISDN terminator on the reporting call agent.

Table 15-10 Call Processing Counters (continued)

Counter Label	Counter Context
CALLP_H323_SS7_CALL	The total number of successfully completed calls from an H.323 originator to an SS7 terminator on the reporting call agent.
CALLP_H323_MGCP_CALL	The total number of successfully completed calls from an H.323 originator to an MGCP terminator on the reporting call agent.
CALLP_H323_CAS_CALL	The total number of successfully completed calls from an H.323 originator to a CAS terminator on the reporting call agent.
CALLP_H323_H323_CALL	The total number of successfully completed calls from an H.323 originator to an H.323 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 hits (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 hits (Reason Code 803) that are received in the DLCX messages on the reporting call agent.
CALLP_NAS_IDLE_TIMEOUT	The total number of idle timeouts (Reason Code 804) that are received in the DLCX messages on the reporting call agent.
CALLP_NAS_SESSION_TIMEOUT	The total number of session timeouts (Reason Code 805) that are received in the DLCX messages on the reporting call agent.
CALLP_NAS_ADMIN_RESET	The total number of adminstrator resets (Reason Code 806) that are received in the DLCX messages on the reporting call agent.
CALLP_NAS_ADMIN_REBOOT	The total number of adminstrator reboots (Reason Code 807) that are received in the DLCX messages on the reporting call agent.
CALLP_NAS_PORT_ERROR	The total number of port errors (Reason Code 808) that are received in the DLCX messages on the reporting call agent.
CALLP_NAS_NAS_ERROR	The total number of NAS errors (Reason Code 809) that are received in the DLCX messages on the reporting call agent.
CALLP_NAS_NAS_REQUEST	The total number of NAS requests (Reason Code 810) 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_REBOOT	The total number of NAS reboots (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 hits (Reason Code 812) that are received in the DLCX messages on the reporting call agent.
CALLP_NAS_PORT_PREEMPTED	The total number of port preempted hits (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 hits (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 hits (Reason Code 815) that are received in the DLCX messages on the reporting call agent.
CALLP_NAS_CALLBACK	The total number of NAS callbacks (Reason Code 816) that are received in the DLCX messages on the reporting call agent.
CALLP_NAS_USER_ERROR	The total number of user errors (Reason Code 817) that are received in the DLCX messages on the reporting call agent.
CALLP_NAS_HOST_REQUEST	The total number of host requests (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 failed 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 failed 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 tests (108) completed by the reporting call agent.
CALLP_TEST_ROUTE_SUCC	The total number of successful TDM loop back tests (108) with DN dialed out in outgoing message completed by the reporting call agent.

Table 15-10 Call Processing Counters (continued)

Counter Label	Counter Context
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.

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 nonacknowledgement 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 nonacknowledgement 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 nonacknowledgement 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 nonacknowledgement messages received by the reporting call agent.
MGCP_RQNT_TX	The number of MGCP RQNT messages sent by the reporting call agent.
MGCP_AUEP_ACK_RX	The number of MGCP AUEP acknowledgement messages received by the reporting call agent.

Table 15-11 MGCP Adapter Counters

Counter Label	Counter Context
MGCP_AUEP_NACK_RX	The number of MGCP AUEP nonacknowledgement 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.
MGCP_AUCX_ACK_RX	The number of AUCX ACK (audit connection acknowledgement) messages that were received by the reporting call agent.
MGCP_AUCX_NACK_RX	The number of AUCX NACK (audit connection nonacknowlegement) messages that were received by the reporting call agent.

Session Initiation Protocol Counters

Table 15-12 identifies the Session Initiation Protocol counters. 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.
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.

Table 15-12 Session Initiation Protocol Counters (continued)

Counter Label	Counter Context
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 acknowledgement messages the reporting call agent or feature server received.
SIS_ACK_TX	The number of SIP acknowledgement 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 informational messages the reporting call agent or feature server received.
SIS_INFO_TX	The number of SIP informational 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.
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.

Table 15-12 Session Initiation Protocol Counters (continued)

Counter Label	Counter Context
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.
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.

Cisco BTS 10200 Status

The Cisco BTS 10200 status (BTSSTAT) software utility provides status information for the entire Cisco BTS 10200 system. It can run on any Cisco BTS 10200 host and report the status of all the network elements in the Cisco BTS 10200 system, including those not on the same host. BTSSTAT is designed to be fast and secure.

The operator can execute the **btsstat** command from the UNIX shell on any host of a Cisco BTS 10200 system. The operator can be any valid UNIX user.

The output of BTSSTAT includes the network element id, side, host name, version, replication status, and redundancy status of all Cisco BTS 10200 network elements. All of the results appear in one screen. A sample of the output is shown in Table 15-13.

Table 15-13 Sample BTSSTAT Output

```
prica16# btsstat
 ------------------------------------------------------------------------
| ID-SIDE (HOST)  | CA146-A(prica16)            | CA146-B(secca16)            |
| VERSION         | 900-05.00.00.I06            | 900-05.00.00.I06            |
| RED, REPL STATE | STANDBY, Replicating        | ACTIVE, Replicating         |
|-----------------+-----------------------------+-----------------------------|
| ID-SIDE (HOST)  | FSAIN205-A(prica16)         | FSAIN205-B(secca16)         |
| VERSION         | 900-05.00.00.I06            | 900-05.00.00.I06            |
| RED, REPL STATE | ACTIVE, Replicating         | STANDBY, Replicating        |
|-----------------+-----------------------------+-----------------------------|
| ID-SIDE (HOST)  | FSPTC235-A(prica16)         | FSPTC-B(secca16)            |
| VERSION         | 900-05.00.00.I06            |                             |
| RED, REPL STATE | ACTIVE, Not Replicating     | No response/OOS             |
|-----------------+-----------------------------+-----------------------------|
| ID-SIDE (HOST)  | EM01-A(priems16)            | EM01-B(secems16)            |
| VERSION         | 900-05.00.00.I06            | 900-05.00.00.I06            |
| RED, REPL STATE | ACTIVE, Replicating         | STANDBY, Replicating        |
|-----------------+-----------------------------+-----------------------------|
| ID-SIDE (HOST)  | BDMS01-A(priems16)          | BDMS01-B(secems16)          |
| VERSION         | 900-05.00.00.I06            | 900-05.00.00.I06            |
| RED, REPL STATE | ACTIVE, Replicating         | STANDBY, Replicating        |
 ------------------------------------------------------------------------
prica16#
```

By default, BTSSTAT relies on /etc/opticall.cfg to find the host name for each Cisco BTS 10200 network element, and uses the default TCP port numbers of the Platform Application Services (PAS) server (Table 15-14) on each side of the network element to establish an SSL connection to it and to obtain information.

Table 15-14 Default TCP Port Number of PAS Server

Application	Default Port Number
CA	16001
FSAIN	16002
FSPTC	16003
EMS	16004
BDMS	16005

Note Both sides of one Cisco BTS 10200 network element use the same port.

You can run BTSSTAT from a host that is not a Cisco BTS 10200, provided that the host can establish an SSL connection to the target Cisco BTS 10200 host. In this case, the Cisco BTS 10200 hosts should be specified in a configuration file. Users can specify a configuration file with the -f option as follows:

```
btsstat -f my_cfg_file
```

The user-provided configuration file must contain the tokens in Table 15-15 along with the values of the corresponding host names. BTSSTAT ignores all other lines in the file.

Table 15-15 BTSSTAT Configuration File Format

Element	Setting
CA_SIDE_A_HN = CA_SIDE_B_HN =	prica11 secca11
FSAIN_SIDE_A_HN = FSAIN_SIDE_B_HN =	prica11 secca11
FSPTC_SIDE_A_HN = FSPTC_SIDE_B_HN =	prica11 secca11
EMS_SIDE_A_HN = EMS_SIDE_B_HN =	priems11 secems11
BDMS_SIDE_A_HN = BDMS_SIDE_B_HN =	priems11 secems11

You can use a command-line argument to specify nondefault port numbers to status for any of the Cisco BTS 10200 network elements. The command-line options in Table 15-16 are for specifying the port numbers.

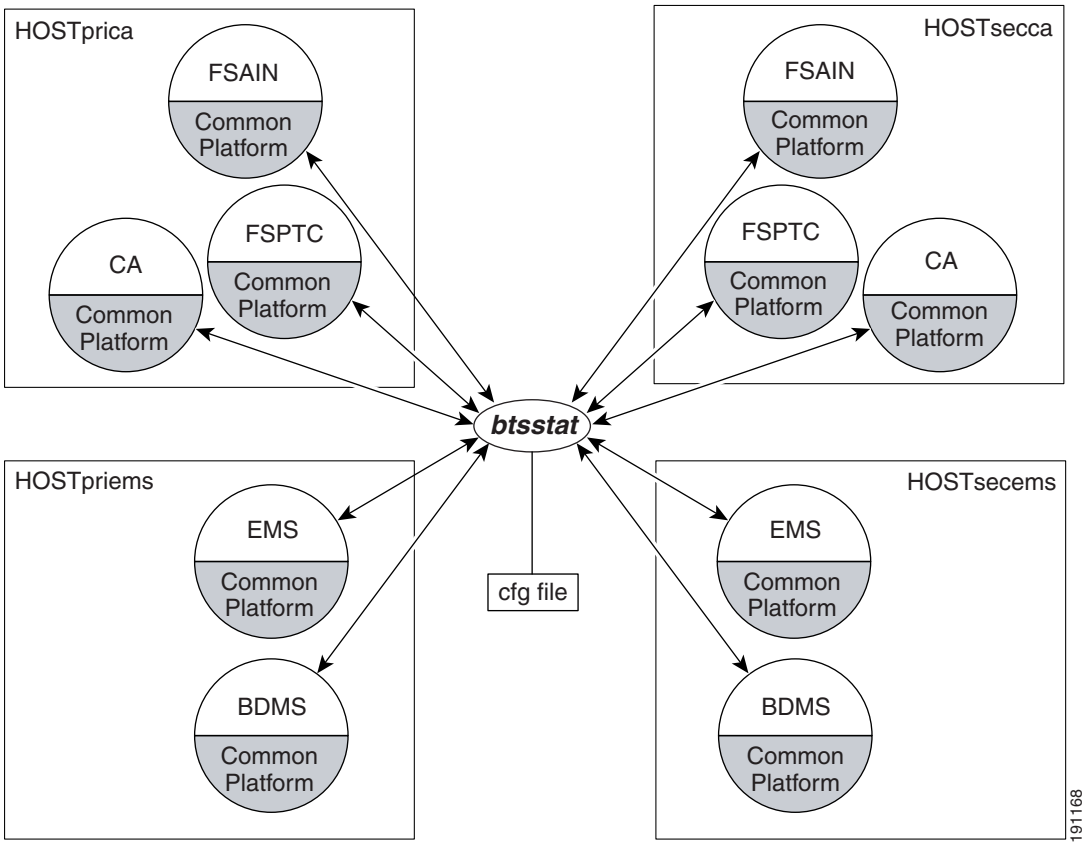
Table 15-16 BTSSTAT Command-line Options for Specifying Port Numbers for Statusing

Command Line Option	Description	Example
-caport <num>	Specify the port number for CA	btsstat -caport 16007
-fsainport <num>	Specify the port number for FSAIN	btsstat -fsainport 16008
-fsptcport <num>	Specify the port number for FSPTC	btsstat -fsptcport 16009
-emsport <num>	Specify the port number for EMS	btsstat -emsport 16010
-bdmsport <num>	Specify the port number for BDMS	btsstat -bdmsport 16011

System Context for BTSSTAT

BTSSTAT queries all the network elements in the same Cisco BTS 10200 system for the status information shown in Figure 15-1. Additionally, Figure 15-1 illustrates the interrelated conditions or context for which the **btsstat** command provides status. BTSSTAT can run on any of these Cisco BTS 10200 hosts, or it can run on a separate host.

Figure 15-1 BTSSTAT System Context



Prerequisites

The BTSSTAT software utility needs Apache xerces-c library Version 2.6.0 or higher to parse and serialize the XML message. This shared library must be present in the host in order for you to run BTSSTAT.

Installing

Use the following procedures to install the BTSSTAT software utility on a Cisco BTS 10200 host and on a host that is not a Cisco BTS 10200.

Installation on a Cisco BTS 10200 Host

BTSSTAT is part of BTSTOOLS package. This package is installed automatically when you install Cisco BTS 10200. The tool is in the /opt/bts/bin directory after installation.

No specific installation/upgrade/fallback procedure is required for this tool.

Installation on a Host That Is Not a Cisco BTS 10200

To install BTSSTAT on a host that is not a Cisco BTS 10200:

Step 1 Make sure that the host is Solaris-SPARC based and that the SSL connection from the host to the target Cisco BTS 10200 system is allowed.

Step 2 Obtain the BTSSTAT executable file and the XML parser library.

On an installed Cisco BTS 10200 system, the two files are located at /opt/bts/bin/btsstat and /opt/BTSlib/lib/libxerces-c.so.26.

Step 3 Transfer the two files into the host that is not a Cisco BTS 10200.

Step 4 Make sure that the BTSSTAT file has the correct permissions and that the library file libxerces-c.so.26 is in $LD_LIBRARY_PATH.

Step 5 Provide your own configuration file (see Table 15-15).

Step 6 Now the **btsstat** command can be run as
btsstat -f cfg_file

For upgrade, the two files can be simply overwritten.

For fallback, the two files can be simply replaced by the previous version.

Call Tracer (CTRAC)

The Cisco BTS 10200 call tracer (CTRAC) feature provides a mechanism that uniquely marks each Cisco BTS 10200 system call to provide a system call trace troubleshooting capability.

The CTRAC feature provides an easy means to filter out trace log lines that correspond to a specific basic or feature call. The filtering is enabled by a unique CTRAC-ID set unconditionally for every call attempt (at the earliest point in time in call processing) and provides a copy of it to all call-processing modules in the Cisco BTS 10200 (across platforms). The CTRAC-ID is used for logging seamlessly into per-call related trace lines corresponding to the call.

Because every per-call related trace log line has a CTRAC-ID, a user can use UNIX **grep** or a similar command to filter out the lines of interest using the CTRAC-ID.

Restrictions and Limitations

Note This feature is available only to users with both CLI and root (UNIX) access.

Due to implementation limitations, it is possible that some per-call related trace logs may not have CTRAC-IDs. Such occurrences however are limited in number.

The CCB shared memory used by various modules is affected. The CCB structure to is expanded include CTRAC-ID.

Operating

The CTRAC feature is the key enabling feature for the end user interested in troubleshooting or debugging calls by viewing the Cisco BTS 10200 trace logs. CTRAC enables the system user to collect all Cisco BTS 10200 trace logs pertaining to a single call. Please refer to the following sections for examples of using the Cisco BTS 10200 CTRAC feature:

- Isolating Calls Based on Billing Record, page 15-86
- Isolating Calls Based on a Given Originating End Point, page 15-86
- Isolating Calls Based on a Given Terminating End Point, page 15-87
- Isolating Calls Which Show Internal Symptoms of Problems, page 15-87

Isolating Calls Based on Billing Record

To isolate calls based on the billing record, take the following steps:

Step 1 For a given call of interest, note (through CLI) the value of the CTRAC-ID billing record parameter. This value is the CTRAC-ID for the call. For this example, assume that it is M0000001. The CTRAC billing-cdr parameter is CTRACID. It can be obtained by using the CLI **report billing-record** command.

Step 2 For each call-processing platform of interest (CA, FSPTC, FSAIN, BDMS), go to the directory where the Cisco BTS 10200 trace logs are stored (by default this is the /opt/OptiCall/<platform-instance-name>/bin/logs directory).

Note If the trace log files are zipped by the platform, you have to copy the zipped files to a separate directory and perform the necessary operations to unzip the file in the separate directory.

```
$ cd /opt/OptiCall/<platform-instance-name>/bin/logs
```

Where platform-instance-name could be CA146, FSPTC235, or the name of some other platform installed in your system.

Step 3 In the directory where the Cisco BTS 10200 trace logs are available, use the UNIX **grep** command to filter out the trace logs corresponding to the selected CTRAC-ID.

```
$  grep "M0000001" *.log > CTRAC-M0000001.txt
```

Step 4 View the CTRAC-M0000001.txt file with a text editor to browse the trace log file lines corresponding to the call.

Isolating Calls Based on a Given Originating End Point

To isolate calls based on a given originating end point, take the following steps:

Step 1 Go to the desired target platform log directory.

```
$ cd /opt/OptiCall/<platform-instance-name>/bin/logs
```

Step 2 Use the UNIX **grep** command to scan for a line of specified format to filter out the term-id/idx to the CTRAC-ID correlation log line.

```
$ grep "OHALF_CTRAC_MAP" | grep "my-term-id-here"
```

The information in the resultant line correlates with the CTRAC-ID for all calls that originated from the specified endpoint.

Step 3 Use the CTRAC-ID to filter out the trace log lines from the Cisco BTS 10200 logs.

Isolating Calls Based on a Given Terminating End Point

To isolate calls based on a given terminating end point, take the following steps:

Step 1 Go to the desired target platform log directory.

```
$ cd /opt/OptiCall/<platform-instance-name>/bin/logs
```

Step 2 Use the UNIX **grep** command to scan for line of specified format to filter out the term-id / idx to CTRAC-ID correlation log line.

```
$ grep "THALF_CTRAC_MAP" | grep "<my-term-id-here>"
```

The information in the resultant line correlates with the CTRAC-ID for all calls that terminated at the specified endpoint.

Step 3 Use the CTRAC-ID to filter out the trace log lines from the Cisco BTS 10200 logs.

Isolating Calls Which Show Internal Symptoms of Problems

To use error and warn messages isolate calls which show internal symptoms of problems, take the following steps:

Step 1 Go to the desired target platform log directory.

```
$ cd /opt/OptiCall/<platform-instance-name>/bin/logs
```

Step 2 Use the UNIX **grep** command to scan for lines with error or warn messages.

```
$  grep "ERROR" *.log
```

Step 3 If you find a nonzero CTRAC-ID present in the appropriate column in the trace log, it means that the error occurred while a call was being processed. Note the CTRAC-ID.

Step 4 Use the CTRAC-ID to filter out the trace log lines from the Cisco BTS 10200 logs.

Billing Fields

The billing record contains a new parameter that contains the CTRAC-ID related to the feature described in this document. The CTRAC billing CDR parameter is named CTRACID.

Troubleshooting

The Cisco BTS 10200 CTRAC feature is intended as a troubleshooting enabler. No specific troubleshooting steps are required other than the use of **grep** to filter out the trace lines corresponding to a CTRAC-ID.

Tabular Display of Events and Alarms

The Cisco BTS 10200 tabular display of events and alarms feature enables the Cisco BTS 10200 to display current alarms, alarm history and event history in tabular form. The underlying CPI layer modification will easily facilitate other commands to display their data in tabular form.

The Cisco BTS 10200 tabular display of events and alarms feature enables the Cisco BTS 10200 to display current alarms, alarm history and event history in tabular form. The output of the **show alarm** and the **show alarm-log** commands will provide a tabular output consisting of one alarm per row. Each of the reported fields will be columns in the tabular output. This will make the outputs much more conducive to capture and printing.

CPI layer changes will facilitate the tabular display of alarms. The CPI layer changes will allow the tabular display of other data through derived request managers.

Operating

There are three new CLI commands related to the Cisco BTS 10200 tabular display of events and alarms feature correlating to the following:

- Show current alarms in tabular format
- Show alarms history in tabular format
- Show events history in tabular format

CLI Commands

The following are show tab CLI commands and their description:

- **show tab-alarm**—Shows current alarms in tabular format
- **show tab-alarm-hist**—Shows alarms history in tabular format
- **show tab-event-hist**—Shows event history in tabular format

An example of the output of executing of one the three commands follows:

```
CLI> show tab-alarm

ID            TYPE          NUMBER   Severity   TIMESTAMP              COMPONENT-ID
12331874656   SIGNALING     68       MAJOR      2005-11-20 11:00:00    testing@mgw_id
12331874657   MAINTENANCE   3        MAJOR      2005-11-20 11:01:00    testing
12331874658   OSS           9        MINOR      2005-11-20 11:02:45    unixserver
12331874659   OSS           9        MINOR      2005-11-20 11:02:45    skittles
```

Prior to Manual Switchover Switch Integrity Diagnostic Utility

This section describes the prior to manual switchover switch integrity diagnostic utility feature that provides the switchover target system health information. For costly traffic outages to be avoided, the switchover decision must be made based on the system health information. The diagnostic script utility automates the manual procedures that are used to collect, check, and verify system health information.

The Cisco BTS 10200 prior to manual switchover switch integrity diagnostic utility feature provides the system health information for the switchover target so that Cisco BTS 10200 customers can decide if they want to perform manual switchover.

The customer service provider operation organizations often periodically perform switch overs during maintenance windows (after midnight and early in the morning). Doing so ensures that the mate system is functional and cleans up any abnormalities that might have accumulated in the current active/primary system (for example, memory leaks, hung processes).

In order to facilitate the switchover operational practice, the Cisco BTS 10200 prior to manual switchover switch integrity diagnostic utility feature provides a diagnostic tool/utility that allows the operator to verify the operational status of the standby system/platform and decide whether it is in a ready state for a switchover.

Note See the *Cisco BTS 10200 Softswitch Network and Subscriber Feature Descriptions, Release 6.0.3* guide for a complete list of subscriber features supported by the Cisco BTS 10200.

Application Status Check

Before performing a manual switchover, you need to ensure that the switchover target is in the standby state. The primary target of the utility is CA application, the utility also checks FS applications to verify that all three applications (CA, FSPTC, and FSAIN) are either all active or all standby.

Because the CA/FS node is likely to be in a “mixed” state, the utility script and the CLI command checks a specific switchover target or all three applications using an optional argument.

Database Check

The Cisco BTS 10200 prior to manual switchover switch integrity diagnostic utility feature performs the following tasks to check database synchronization, replication, and shared memory integrity.

1. Audit the DB to check for a mismatch between the EMS and the CA.
2. Query for the following DB replication related alarms:

Type and Number	Description	Severity
Database (3)	There Are Errors in Element Management System Database DefError Queue; Contact Database Administrator (There are Errors in EMS Database DefError Queue; Contact DBA)	Critical
Database (4)	Element Management System Database HeartBeat: Replication Push Job Broken (EMS DB_Heart_Beat: Replication Push Job Broken)	Critical
Database (5)	Element Management System Database HeartBeat Process Died (EMS DBHeartBeat Process Died)	Critical

3. Run the shared memory integrity tool to validate the shared memory integrity of the CA processes.

System Time Check

The Cisco BTS 10200 prior to manual switchover switch integrity diagnostic utility feature queries the system for the following alarms to see there is any system time drift.

Type and Number	Description	Severity
Audit (11)	Critical Network Time Protocol Service Failure (Critical NTP Service Failure)	Critical
Audit (12)	Major Network Time Protocol Service Failure (Major NTP Service Failure)	Major
Maintenance (77)	Mate Time Differs Beyond Tolerance	Major

Switchover Impact Alarms Check

The Cisco BTS 10200 prior to manual switchover switch integrity diagnostic utility feature queries the database for the following alarms to see if they are being raised by the switchover target side. A complete listing of these outstanding alarms is stored in a log file.

Type and Number	Description	Severity
Call Processing (12)	Feature Server Both Links Down	Critical
Maintenance (50)	Index Table Usage Exceeded Critical Usage Threshold Level (IDX Table Usage Exceeded Critical Usage Threshold Level)	Critical
Maintenance (53)	The Central Processing Unit Usage is Over 90% Busy (The CPU Usage is Over 90% Busy)	Critical
Maintenance (55)	The Five Minute Load Average is Abnormally High	Major
Maintenance (57)	Memory and Swap are Consumed at Critical Levels	Critical
Maintenance (61)	No Heartbeat Messages Received Through the Interface (No HB Messages Received Through the Interface)	Critical
Maintenance (62)	Link Monitor: Interface Lost Communication	Major
Maintenance (63)	Outgoing Heartbeat Period Exceeded Limit (Outgoing HB Period Exceeded Limit)	Major
Maintenance (64)	Average Outgoing Heartbeat Period Exceeds Major Alarm Limit (Average Outgoing HB Period Exceeds Maj Alarm Limit)	Major

Type and Number	Description	Severity
Maintenance (65)	Disk Partition Critically Consumed	Critical
Maintenance (66)	Disk Partition Significantly Consumed	Major
Maintenance (68)	The Free Inter-Process Communication Pool Buffers Below Major Threshold (The Free IPC Pool Buffers Below Major Threshold)	Major
Maintenance (69)	The Free Inter-Process Communication Pool Buffers Below Critical Threshold (The Free IPC Pool Buffers Below Critical Threshold)	Critical
Maintenance (70)	The Free Inter-Process Communication Pool Buffer Count Below Minimum Required (The Free IPC Pool Buffer Count Below Minimum Required)	Critical
Maintenance (82)	Average Outgoing Heartbeat Period Exceeds Critical Limit (Average Outgoing HB Period Exceeds Critical Limit)	Critical
Maintenance (84)	Swap Space Below Major Threshold	Major
Maintenance (85)	Swap Space Below Critical Threshold	Critical
Maintenance (107)	No Heartbeat Messages Received Through Interface From Router (No HB Messages Received Through Interface From Router)	Critical
Signaling (109)	Stream Control Transmission Protocol Association Failure (SCTP Association Failure)	Major
Signaling (113)	Signaling Gateway Failure	Major
Signaling (114)	Signaling Gateway Process is Out-of-Service	Major
Signaling (121)	Message Transfer Part 3 User Adapter Cannot Go Standby (M3UA/SUA Cannot Go Standby)	Major

Inter-Node Communication Check

The Cisco BTS 10200 prior to manual switchover switch integrity diagnostic utility feature performs the following communication status checks on all four nodes:

- Checks if internode communication links are established
- Checks if hub is communicating
- Checks if EMS and CA can communicate
- Checks if EMS and feature server can communicate

Process Configuration Check

The Cisco BTS 10200 prior to manual switchover switch integrity diagnostic utility feature queries the system for the following alarms to see if there are any feature server configuration errors.

Type and Number	Description	Severity
Configuration (5)	Feature Server Database and Command Line Host Mismatch (Feature Server DB and Command Line Host Mismatch)	Minor

Operating System Issues in /var/adm/messages Check

The Cisco BTS 10200 prior to manual switchover switch integrity diagnostic utility feature checks /var/adm/messages for any operating system errors. The feature searches for the following Solaris event types:

- kern.err
- kern.crit
- kern.em

Software Configuration Check

The Cisco BTS 10200 prior to manual switchover switch integrity diagnostic utility feature checks the following items.

- Verify that the mem.cfg files are identical on primary and secondary EMS nodes
- Verify that the mem.cfg files are identical on primary and secondary CA nodes
- Verify that the patch/version levels are identical on primary and secondary EMS nodes
- Verify that the patch/version levels are identical on primary and secondary CA nodes

Installing

The Cisco BTS 10200 prior to manual switchover switch integrity diagnostic utility feature utility script is packaged with the Cisco BTS 10200 software upgrade automation scripts. The script resides in the /opt/ems/utils directory after the Cisco BTS 10200 software is installed or upgraded. The script output logs are managed by the check log function, which is run periodically as a cron job.

Command Responses

The new **presw-diag** CLI command internally executes the Cisco BTS 10200 prior to manual switchover switch integrity diagnostic utility script. The output of the utility script is displayed as the command response. For security reasons, user input for the password field is masked with asterisks (“*”). The assumption here is that the passwords for of all four Cisco BTS 10200 nodes are identical.

Example:

show presw-diag password=***; [target=appId];

- password field:
  - Root password of the Cisco BTS 10200 nodes
- target field:
  - Is optional parameter, and is used to specify the switchover target.
  - Allowed values are CA, FSPTC, FSAIN.
  - If target field is specified, the mate of the active side of the specified application is checked.
  - If target field is not specified, the mate of the active side of all three applications is checked.

CLI Database

Note We recommend executing the CLI command to utilize the Cisco BTS 10200 prior to manual switchover switch integrity diagnostic utility feature.

The **presw-diag** CLI command internally executes the Cisco BTS 10200 prior to manual switchover switch integrity diagnostic utility script. The output of the utility script is displayed as the command response. For security reasons, user input of the password field is masked with asterisks (“*”). The assumption here us that the passwords for all four Cisco BTS 10200 nodes are identical. All existing commands used with this feature are documented in the Cisco BTS 10200 Softswitch CLI Database.

Script Arguments

The Cisco BTS 10200 prior to manual switchover switch integrity diagnostic utility script will uses an optional argument for specifying the switchover target. Possible argument values are CA, FSPTC, and FSAIN. The usage of this optional argument is the same as that for the **presw-diag** CLI command target field.

Script Output

The Cisco BTS 10200 prior to manual switchover switch integrity diagnostic utility script displays the resulting summary on the screen and also stores detailed information in a log file.

Log File

The script output log file

- Contains a timestamp so that its name is unique
- Is stored in the /opt/ems/log directory on the node that the script utility is running from
- Is managed by the Cisco BTS 10200 log archiving utility

Result Summary

The script utility uses the following format for the result summary. The summary is displayed on the screen and is stored in the log file.

Legend for the possible values:

- boolean: either “Y” or “N”

Switchover target status okay = boolean

EMS and CA DB in sync = boolean

EMS-A and EMS-B DB in sync = boolean

CA shared memory integrity okay = boolean

System time in sync = boolean

No switchover impact alarms = boolean

Process configuration okay = boolean

Inter-node communication okay = boolean

No issues in OS messages file = boolean

Cisco BTS 10200 software configuration okay = boolean

Log file = [logFileName]

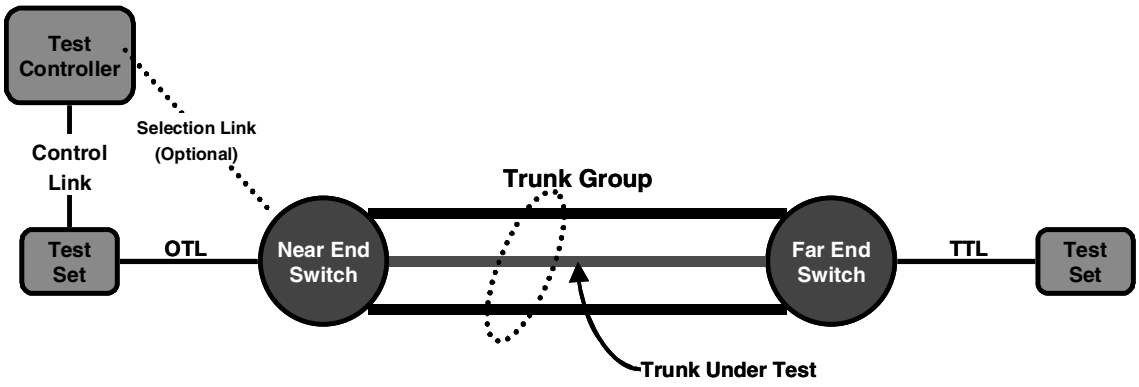
PSTN Trunk Testing

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 15-2 depicts a typical trunk test system.

Figure 15-2 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

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 15-3 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 15-3 shows the format when the OTL is configured for MF signaling.

Figure 15-3 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	KP	Trunk Group Number				Member Trunk				1	0	0	ST						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 15-4. Since the digits may be sent by SS7, MF, or DTMF, only the actual destination digits are depicted.

Figure 15-4 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

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 15-5. 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 15-5 958-11XX 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

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 15-6. Since the digits might be sent through SS7, MF, or DTMF, only the actual destination digits are depicted.

Figure 15-6 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

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 15-7.

Figure 15-7 958-11XX 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

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 15-2.
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: August 10, 2011, OL-25016-01

Introduction

This chapter tells you 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.

We recommend 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 back up 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 back up 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 system. The flash archive back up 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, it is best 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 http://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 We recommend running this procedure during a 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 and 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> and press **Esc-2** to continue.

Step 13 Enter <IP address> and 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> and 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 and then press **Esc-4**.

Step 28 Choose **Manual reboot** and 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
```

Step 31 Mark **x** on primary Disk and then Press **Esc-2**.

Step 32 Press **Esc-2** to continue without preserving data.

Step 33 Press **Esc-4** for Customize disk layout.

Step 34 Partition the disk as follow 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 takes about 15–30 minutes.

Step 38 Press "!" (exclamation 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 Log in 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 system:

```
shutdown -y -g0 -i6
```

Restoring the Cisco BTS 10200 Application

To restore the software application, perform the following steps:

Step 1 Log in 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 Cisco BTS 10200 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 We recommend running this procedure during a maintenance window or when traffic is low.

Power Failure Recovery

One critical component of the Cisco BTS 10200 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 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. Check and analyze the logs for details that may provide the cause of the failure.

Power Failure Scenarios

Four power failure scenarios are discussed in the following sections:

- Power Failure on Single Host Computer, page 16-8

  Only one host of the two mated host computers is affected by the power outage.

- Power Failure on Both Call Agent Computers, page 16-9

  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 16-10

  All host 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 current state of the mate to the host computer, the following procedure discusses 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. 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 CLI Database 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 Fix discrepancies by means of 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 be no 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 Fix discrepancies using 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 be no 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 call agent 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 CLI Database.

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 Fix discrepancies using 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 be no single point of failure in the power feeds.

Element Management System Database Recovery From Hot Back Up

This section provides procedures you can use to restore your Oracle EMS database data files from the most current hot back up and then recover your database from the back up. If additional archive log back up (by ora_arch_backup.ksh) was done after the hot back up, the additional archive log back up file sets need to be restored also. All of these back up file sets are assumed to be located on the remote FTP site.

Directory to restore back up files: /opt/oraback.

The following assumptions were made for this procedure:

Daily back up schedule:

2:00 AM–daily hot back up (by ora_hot_backup.ksh process)

18:00 PM–daily archive log back up (by ora_arch_backup.ksh process)

Oracle databases on both primary and secondary EMS systems crashed completely at January 10, 2007, 20:00pm.

Recovery Goal

The goal in the scenario above is to recover the primary EMS Oracle database by using your most recent back ups.

In this case, since the database crashed January 10, 2007, 20:00pm, the back up file sets with timestamp '200701100200' from 2:00am hot back up and those with timestamp '200701101800' from 18:00 archive log back up must be restored. Timestamp is formatted as YYYY:MM:DD:hh:mm.

If your database crashes before the archive log back up, you need to restore only the 2:00 am hot back up file sets.

If your system does not perform extra archive log back up daily by ora_arch_backup.ksh, use back up file sets from hot back up only.

In this sample scenario, the primary EMS database is 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 back up 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 fully populated with data; each archive log file requires 5 MB additional space. The number of archive log files in the back up 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 back up file sets from the remote FTP site.

FTP the targeted database back up 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 archive log back up is not performed, get only the hot back up files.

Back up files from 2:00 hot back up:

- optical1_arc_full_1_167:200701100200.Z
- optical1_arc_full_1_168:200701100200.Z
- optical1_ctl_binary: 200701100200.Z
- optical1_ctltrc:200701100200:tar.Z
- optical1_hot_full_1_166:200701100200.Z
- optical1_ora_hot_full_backup_200701100200.log

Back up files from the 18:00 archive log back up:

- optical1_arc_incr_1_169:200701101800.Z
- optical1_ctl_binary:200701101800.Z
- optical1_ctltrc:200701101800:tar.Z
- optical1_ora_arc_incr_backup_200701101800.log

```
ftp> prompt
```

```
ftp> mget optical1*200701100200*
ftp> mget optical1*200701101800*
ftp> quit
ls *200701100200*
ls *200701101800*
```

f. Uncompress your files:

```
uncompress *200701100200*.Z
uncompress *200701101800*.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 back up.

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 back up.

Step 8 Restore the back up binary control file to the database target directories:

Use the most current back up binary control file. In this case use the optical1_ctl_binary:200701101800 file from 18:00pm archive log back up. If archivelog back up was not restored use the binary control file from 2:00am back up. Copy the back up binary control file to both db1/control01.dbf and db2/control02.dbf files.

```
cp /opt/oraback/optical1_ctl_binary:200701101800 db1/control01.ctl
cp /opt/oraback/optical1_ctl_binary:200701101800 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 back up to temp tablespace. When this script is completed successfully, database is recovered to the point of time of the back ups.

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_200701101636.log

<Thu Jan 10 16:36:51 CST 2007> ./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 2007> All datafiles are restored.

<Thu Jan 10 16:40:15 CST 2007> Begin to recover database.

Recover database until time '20070111 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_200701101636.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 2007> Database recovery ended.

<Thu Jan 10 16:44:27 CST 2007> Alter database open resetlogs
Connected.
Database altered.
….
Database is successfully recovered.

<Thu Jan 10 16:44:38 CST 2007> ./recover_db_until_time.ksh ended.
```

Post Recovery–Cold Back Up

Once you have recovered your database, you need to make a cold back up of the database using the **dbadm –E cold_backup** command. The following tar files are created from the cold back up 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 off site 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 back up is completed, save a copy of the back up files to the */opt/oraback* directory for the ftp script to transfer off site.

```
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/*200701100200*
ls /opt/oraback/*200701101800*

rm /opt/oraback/*200701100200*
rm /opt/oraback/*200701101800*
```

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" section on page 16-17.

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 one of the two 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, log in 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 reinstallation is not required, go to Step 5 to reload the database from the database back up file. Continue to Step 6.

Option 2 If the entire system is corrupted and flash archive system back up is available, recover the system from the flash archive, as detailed in the "Flash Archive Restore" section on page 16-2. The flash archive back up file should have the Cisco BTS 10200 applications included. Continue to Step 6.

Option 3 If the entire system is corrupted and the flash archive back up file is not available, you must jump start the system, and reinstall the Cisco BTS 10200 software from the installation CD, as shown below, "Reinstalling the Cisco BTS 10200 Software on the Corrupted EMS" section on page 16-19.

Reinstalling the Cisco BTS 10200 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 back up to the corrupted EMS site.

If the EMS system is intact, but only the Oracle database is corrupted, you can use the cold back up tar file to restore the database data files. The cold back up 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 back up tar file.

Note If there is no cold back up database tar file, you can restore database from hot back up. Refer to the "Element Management System Database Recovery From Hot Back Up" section on page 16-11 to recover your database from hot back up.

a. Restore the database from the cold back up 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 restored, 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 to the following 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:

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 CLI Database 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, the command 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 CLI Database 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 3 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" section on page 16-31.

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 created through the CLI commands listed in Table 16-1.

Table 16-1 Controlling Trunks and Trunk Groups Examples

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 is placed in the /opt/OptiCall/CAxxx/bin directory on the primary CA.

The cs-control script is invoked from the /opt/OptiCall/CAxxx/bin directory to place subscribers in-service as follows:

cs-control data *<name of the script used in the step above>*

Shared-Memory Synchronization

Prior to the Shared-Memory Synchronization feature implementation, the data contained in the shared memory (provisioned and dynamic data) of the Cisco BTS 10200 network elements (CA, FS, and so forth) was not periodically written reliably to disk. Because of this, if a power outage occurred and the power was restored, the Cisco BTS 10200 network could come back up on stale data. This could result in loss of service at a customer site, due to loss of provisioned data. Previously, synchronization occurred only at the time of manual platform shutdown.

The Cisco BTS 10200 Shared-Memory Synchronization (SMS) feature adds a periodic synchronization of the shared memory to the disk. If a power cycle happens, the loss of data is limited to the changes since the last sync.

The Shared-Memory Synchronization feature provides the ability to periodically perform a sync of the shared memory to disk at a pre-determined interval. After a power failure, the system will automatically come back up with data from the last sync minimizing data loss.

Troubleshooting

The links below indicate how to troubleshoot the following conditions:

- Periodic Shared Memory Sync Started—Maintenance (124)
- Periodic Shared Memory Sync Completed—Maintenance (125)
- Periodic Shared Memory Sync Failure—Maintenance (126)

Incremental Shared-Memory Restoration

This section describes the Incremental Shared-Memory Restoration (ISMR) feature for Release 6.0 of the Cisco BTS 10200 Softswitch and explains how to use it. The ISMR feature is part of an operational solution that addresses comprehensive recovery from disastrous system incidents like an abrupt power-cut.

The ISMR feature represents a means to recover the Cisco BTS 10200 shared-memory (SHM) on a platform by bringing it back to the state where it was at the time of a system disaster (ex.: power-cut). The Cisco BTS 10200 ISMR works in conjunction with the Cisco BTS 10200 ASMB (Automated Shared-Memory Backup) feature, which restores all of the BTS 10200 shared-memory contents to a point-in-time of the latest SHM backup. However, several provisioning and control commands (incremental commands) might have changed the contents of the SHM after the latest periodic backup. An audit/sync step after an ASMB operation could take considerable time if the incremental commands are not applied in the database in an efficient manner.

The ISMR feature working in conjunction with the Shared-Memory Synchronization (SMS) feature bridges the gap in SHM between the latest backup snapshot and disaster-moment snapshot in an extremely efficient manner. When the disaster-moment snapshot is restored, post-ASMB-backup commands restored, the Cisco BTS 10200 restarted, and EMS database audited/synchronized, the system is ready to restart operations from a system internal disaster incident.

The ISMR feature provides:

- A comprehensive solution for automatic ongoing logging of Post-Backup Incremental Commands (PBIC) (such as provisioning and control commands that were affected in the SHM after latest successful backup).
- A configurable manual incremental restoration of SHM using the incremental commands.

- A best-effort solution with the no specific time constraints. The time for the ISMR to complete depends on the number of PBICs present in the system.
- A complete snapshot of the SHM in conjunction with SMS feature.
- The ISMR feature consists of the following logical components:
- Recording—The recording component of ISMR feature is responsible to continuously intercept and log the provisioning and control command in a redundant manner to the ISMR log archive.
- Editing—The editing component of ISMR feature is responsible for sequencing, filtering and formatting an ISMR log file in such a manner that is ready for ISMR replay. The original recording will have certain annotations that need to be filtered out.
- Playback—The playback component of ISMR feature, which is activated after an ASMB restore, is responsible for performing the necessary editing of the ISMR log archive and for using the logged commands to restore provisioning into the applicable shared memory.

Feature Interactions

The ISMR feature works in conjunction with the ASMB feature and the SMS feature.

Prerequisites

The ASMB feature is a prerequisites for the ISMR feature.

Assumptions

The ISMR feature implementation assumes that all mated-pair Cisco BTS 10200 network-elements work within the same time-zone.

Operating

This section explains how to perform operational tasks for the ISMR feature.

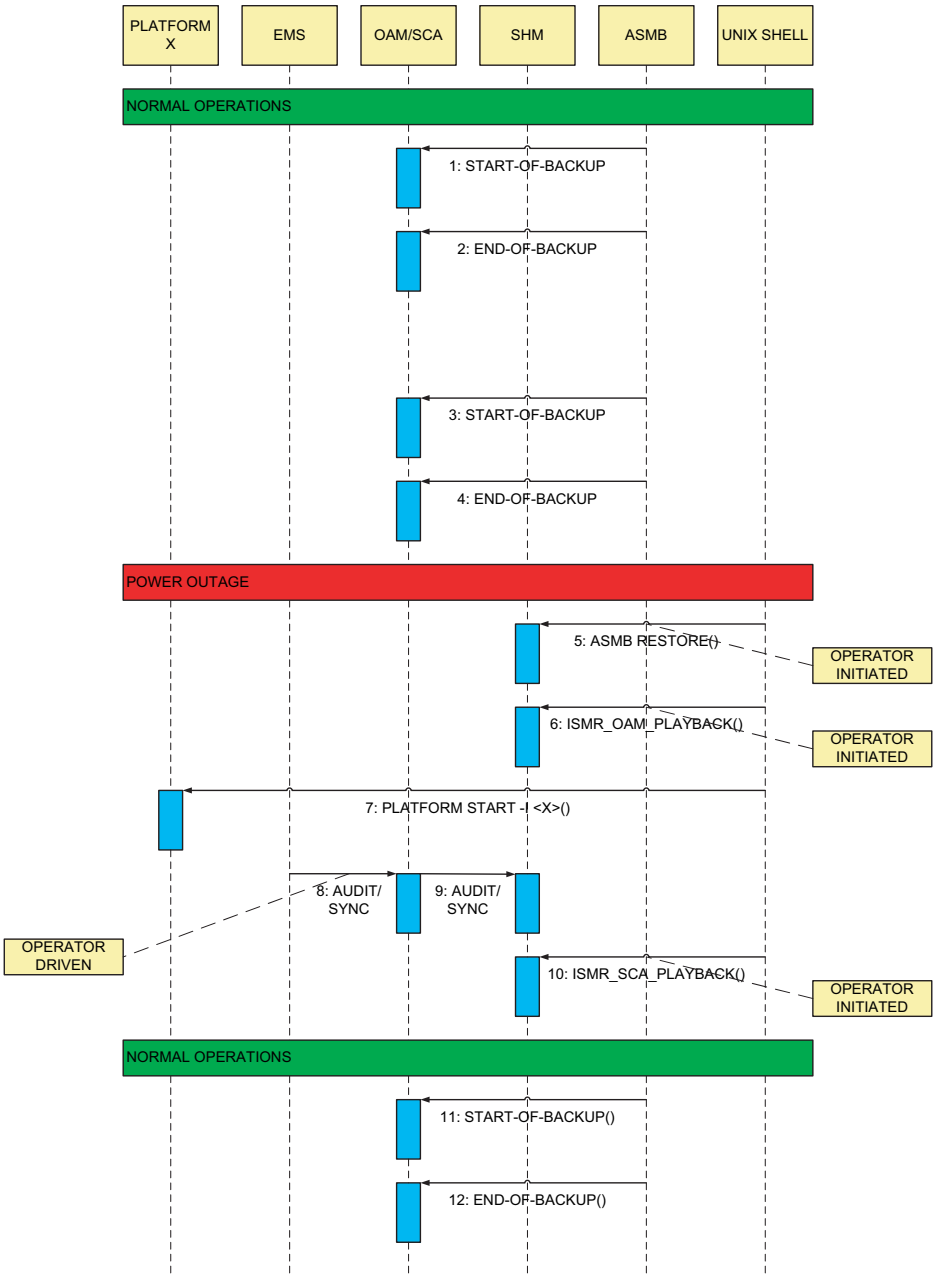
- Recovery Operations
- Single Platform Disaster Operations
- Multi-Platform Disaster Operations

Recovery Operations

The ISMR recovery operations are shown in Figure 16-1. As a convention, the "()" shown along side tasks in Figure 16-1 implies a predefined set of sub-procedures.

Note Since at the time of ISMR playback the platform is *not* supposed to be up, there is no active/standby classification. The ISMR provisioning playback should work on either side during this phase. Once the platform is up, ISMR playback will only work on the active side.

Figure 16-1 Comprehensive Shared Memory Backup and Restoration - Operations



Single Platform Disaster Operations

When a single Cisco BTS 10200 platform encounters a disastrous condition resulting in SHM corruption, the following ISMR operational procedures must be followed in order to comprehensively recover from the disaster or SHM corruption:

Step 1 Perform the operational steps recommended for the ASMB feature.

Step 2 Execute the **ISMR_prov_playback** command as per its command-line syntax.

Step 3 Perform a platform start.

Step 4 Synchronize SHM database with EMS by use of the CLI audit or sync facility.

Step 5 Execute the **ISMR_ctrl_playback** command as per its command-line syntax.

The Cisco BTS 10200 SHM should now be the same as the post disaster-moment snapshot.

Multi-Platform Disaster Operations

In Table 16-2, a Y in a column indicates that the corresponding platform (in the column header) has been struck with a disaster, while a — indicates normal operation. The fourth column identifies the sequence in which the platforms are restored. The specific recovery steps are noted in the Single Platform Disaster Operations section. If both primary and secondary sides of a network-element are down, it is recommended to recover the primary side first. In order to save time to restore, CA and FS can be restored simultaneously if they are restored on different hosts. EMS restoration must always follow CA/FS restorations.

Table 16-2 Multi-Platform Disaster Operations Matrix

EMS	CA	FS	Recovery Sequence for Platforms
—	—	—	FS **Note** If every platform is normal, recovery sequence of platforms should also be normal (-). If needed, all platforms can be included (CA, FS, EMS not only FS).
—	Y	—	CA
—	Y	Y	CA, FS
Y	—	—	EMS
Y	—	Y	FS, EMS
Y	Y	—	CA, EMS
Y	Y	Y	CA, FS, EMS

To troubleshoot the following condition:

- Secure File Transfer Protocol Transfer Failed—Database (25)

See Secure File Transfer Protocol Transfer Failed—Database (25) section in the *Cisco BTS 10200 Softswitch Troubleshooting Guide*.

Disaster Recovery Using the Automatic Shared Memory Back Up

Note This procedure is for use with Cisco BTS 10200 Release 4.5.1 and above.

This section describes the procedure for restoring a Cisco BTS 10200 network element's shared memory from a back up copy created by the Cisco BTS 10200 Automatic Shared Memory Back Up subsystem.

This procedure should be run only if memory is corrupted in both the active and standby sides of the same Cisco BTS 10200 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 Back Up (ASMB) can be up to 24 hours old. Provisioning done in the time since the back up 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 be completed only if both of the following conditions are true:

- Both Side A and Side B of the same Cisco BTS 10200 network element are out of service.
- Neither side of the same Cisco BTS 10200 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 network element should be restored to the ASMB back up 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 back up for the platform. This back up resides on the system in the /bin directory of each Cisco BTS 10200 network element.

Automatic Shared Memory Back Up Restore

This section describes the procedure for restoring a platform to its ASMB shared memory back up.

It is possible that multiple Cisco BTS 10200 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 system separate from the Call Agent and Feature Servers; therefore, they can be recovered in parallel with the NEs on the CA/FS system.

Additionally, all Cisco BTS 10200 NEs on one of the systems should be restored first before you attempt to restore those on the mate. This ensures that full service is restored as soon as possible.

Note The backup data directory contains shared memory files in the *gunzip* format.

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 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 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 back up can be up to 24 hours old, differences between the two systems are probable. 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 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 back up copy to be used. The ASMB back up 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 back up copy to the data directory for the Cisco BTS 10200 NE being restored.

Automatic Restart

This section describes the Cisco BTS 10200 automatic restart feature. The Cisco BTS 10200 automatic restart feature is beneficial to customers because the Cisco BTS 10200 will attempt to automatically restart a platform (EMS/FS/CA) to standby that has become OOS-faulty and has shut down. Currently the Cisco BTS 10200 will not restart a platform in this situation, leaving the active platform running in a vulnerable simplex mode until the standby platform is restored manually.

Note An automatic restart is not attempted if the restart of the system is likely to fail.

Benefits of this feature:

- Reduced outage risk. Automatic restart–when successful–brings the platform up to standby in minutes instead of potentially much longer, as support personnel work to restore the platform. This reduces the risk of outages by reducing the amount of time the system is in simplex mode.
- Automated forensic data collection. This feature automatically saves data useful for offline debugging (trace logs, status files, cores, and so on). Currently this data is retrieved manually. Automating the process of saving off useful information guarantees that this information is preserved.
- Faster switch overs. When a process exceeds the maximum number of restarts, a system-initiated switchover is executed. By not transitioning to OOS-faulty, the standby side avoids the taxing database copy process.

The processing associated with the Cisco BTS 10200 automatic restart feature has two main phases. In the first phase, the transition is made to OOS-faulty. During this phase, the forensic information for offline analysis must be collected and stored. In the second phase, the attempts are made to bring the platform from OOS-faulty to standby.

Transition to OOS-Faulty

When the platform is transitioning to OOS-faulty, the automatic restart feature requires the additional processing described here.

There is no need to save the alarm log or event log because they are contained in the MySQL database. This database is external to the platform and is not affected by platform shutdowns or bring ups.

The following processes are completed during the transition to OOS-faulty:

- Create /saved.debug Subdirectory—Create the /saved.debug subdirectory.
- Archive the /data Directory—Copy and archive the /data directory and all of its contents to the /saved.debug directory using a tar file with a timestamp in the name.
- Unwritten Traces—Any unwritten, buffered trace memory is saved.
- Save Trace Logs—The most recent trace log files are saved. The number of logs to save is a configurable parameter. This is especially useful when the Automatic Restart feature is active because a system side might only temporarily remain in OOS-faulty. If the system side comes back to a working standby state, it is less urgent that support personnel retrieve logs, and so on. from the node.
- Disk Space for /saved.debug—The disk space consumed by /saved.debug is conserved by deleting the /saved.debug directory and its contents each automatic restart cycle. The saved.debug subdirectory is created in the platform's /bin directory, which is <path>/bin/saved.debug.

Automatic Restart Processing

Automatic restart processing is not always desired, or possible. Table 16-3 lists the platform restart actions for the OOS-faulty state. The restart actions fall into one of three categories:

- SDAMR (Shut Down and Manually Restart)—These scenarios are handled the same way as the OOS-faulty behavior for earlier releases of the Cisco BTS 10200. The platform will shut down and wait for manual restart. All initialization-related processing (bring up) is treated this way.
- SDAAR (Shut Down and Automatically Restart)—These are the scenarios in which an automatic restart is attempted.
- FISS (Fault-initiated Switch to Standby)—In these scenarios, a faster system-initiated switchover is attempted.

The scenarios are grouped into PMG-initiated, KAM-initiated, and application-initiated. PMG and KAM start the vast majority of shutdowns. For PMG-initiated and KAM-initiated, the shutdowns are grouped by the state of the platform.

Table 16-3 OOS-Faulty Behavior

Description	Result
PMG-initiated Shutdowns	
Bringup	
One or more processes did not come up to correct state.[1]	SDAMR
Unable to open log file (/var/adm/events_to_<plat>).	SDAMR
During bring up to active, one or more processes in a bad state.	SDAMR
During bring up to standby, one or more processes in a bad state.	SDAMR
One or more processes in a bad state.	SDAMR
Active	
A crashing process exceeded the restart rate.	See Note[2]
Disk usage exceeded.	SDAMR
Swap space usage exceeded and mate ok.	SDAAR
IPC memory usage exceeded and mate is ok. If mate not ok, no shutdown.	SDAAR
Standby	
A crashing process exceeded the restart rate.	See Note 2
IPC memory usage exceeded and mate is ok. If mate not ok, no shutdown.	SDAAR
Disk usage exceeded.	SDAMR
Swap space usage exceeded and mate ok.	SDAAR
Switchover to Active	
Switchover to active: failed to start all processes in active.	SDAAR
Switchover to standby	
Switchover to standby: failed to start all processes in standby.	SDAAR
All States	
Watchdog expires for a PMG thread–or threads that are not PMG threads handled by restart logic.	SDAAR

Table 16-3 OOS-Faulty Behavior (continued)

Description	Result
When PMG receives a SIGINT.	SDAAR
KAM-initiated Shutdowns	
Bringup	
System time gets out-of-sync with mate when standby comes up.	SDAMR
Network interface is down.	SDAMR
Timer initialization failure.	SDAMR
Configuration error with ip addresses.	SDAMR
Thread creation failed.	SDAMR
Shared memory DB in bad state.	SDAMR
Data replication not enabled to run.	SDAMR
Mate faulty during DB copy.	SDAMR
DB copy fail.	SDAMR
DB clear timeout.	SDAMR
DB copy timeout.	SDAMR
Data replication connection down.	SDAMR
Init thread failed.	SDAMR
HB timer failure.	SDAMR
Time out of sync with mate.	SDAMR
Mate wrong side.	SDAMR
Mate wrong ip address.	SDAMR
Mate standby state.	SDAMR
Mate not active.	SDAMR
Active	
Active–heartbeat failure and mate is OK.	SDAAR
Standby	
Heartbeat with mate not working properly.	SDAAR
Timeout waiting for call data updates completion.	SDAAR
DB copy timeout.	SDAAR
DB copy failed.	SDAAR
Switchover: failed to receive completion acknowledgement.	SDAAR
Unable to establish data replication connection to mate.	SDAAR
While waiting for CRQ, data replication was restarted.	SDAAR
Switchover to Active	
Switchover to active, but failure.	SDAAR
Switchover to active, but timeout failure.	SDAAR
Switchover to active, but RDM restarted.	SDAAR

Table 16-3 OOS-Faulty Behavior (continued)

Description	Result
Switchover to Standby	
Switchover to standby, but failure.	SDAAR
Switchover to standby, but timeout failure.	SDAAR
Switchover to standby, but DB copy failure.	SDAAR
All States	
KAM received a signal.	SDAAR
Application-initiated Shutdowns	
Active	
BMG2 (Billing Manager). Problems parsing command line options.	See Note 2
H3A. When there are no good H3A signaling links.	See Note 2
MGA. When all the needed interfaces are either faulty or not stabilized.	See Note 2
SGA. When both signaling gateways are down.	See Note 2
EPA. When the EMS is not reachable.	See Note 2
NIM. When all of the HUB interfaces are faulty.	See Note 2
Standby	
BMG2 (Billing Manager). Problems parsing command line options.	See Note 2
H3A. When there are no good H3A signaling links.	See Note 2
MGA. When all the needed interfaces are either faulty or not stabilized.	See Note 2
SGA. When both signaling gateways are down.	See Note 2
EPA. When the EMS is not reachable.	See Note 2
NIM. When all of the HUB interfaces are faulty.	See Note 2

1. Most references to process state in this table refer to a platform-internal state assigned to each process. The Process Manager methodically brings up the platform by starting processes in a given sequence. When a process does not reach the proper state at a given point during startup, it is declared to be in a bad/or incorrect state.
2. The shutdown action is specified by the process's platform.cfg parameters: ProcessCriticalFailureActionWhenMateStandby, ProcessCriticalFailureActionWhenMateActive, or ProcessCriticalFailureActionWhenMateFaulty.

The following processes are completed during the automatic restart processing:

- Check if Restart is Possible (Table 16-3)—An intelligent processing to check if a restart should be attempted is completed. The default behavior is to attempt an Automatic Restart the maximum number of configured times.
- platform start/platform stop—The **platform start** and **platform stop** commands do not work when an Automatic Restart is scheduled. However, the user can use the **-noautorestar**t command option on either command to bypass the Automatic Restart and force the platform start or stop to occur immediately.

Installing

There are two customer-provisionable parameters (SystemAutoRestartRate and SystemAutoRestartDelay) and one new platform-provisionable parameter (SystemAutoRestartNumSavedTraceLogs) for the Cisco BTS 10200 automatic restart feature. Additionally, two existing parameters are expanded into three parameters.

Configuring

This section explains how to perform the following tasks:

- Opticall Configuration
- Platform Configuration

Opticall Configuration

The configuration changes for this feature are the new customer-configurable parameters added to the opticall.cfg file. These parameters are listed and discussed here. They are used to control the Automatic Restart feature.

- SystemAutoRestartRate—This variable indicates the number of times a platform auto restart is attempted. This variable is defined to be the number of times a restart shall be attempted over a 30-minute interval.
- SystemAutoRestartDelay—A side that is down should delay by this amount before attempting to restart. The default is 10 minutes. The newly active side is allowed time to begin processing fully before needing to support the auto restart of the faulty side.

Platform Configuration

The following parameter is added to the platform.cfg file.

- SystemAutoRestartNumSavedTraceLogs—This variable indicates the number of most recent consecutive trace logs to save.

The following parameters are changed in platform.cfg file. In earlier releases, theses parameters could be set for each process.

- SwitchOverIfMaxRestartExceededInDuplex = [yes | no]
- EndPlatformIfMaxRestartExceededWhenMateFaulty = [yes | no]

To support the Automatic Restart feature, these two parameters are replaced with the following three parameters.

- ProcessCriticalFailureActionWhenMateStandby = [NONE | SDAMR | SDAAR | FISS]
- ProcessCriticalFailureActionWhenMateActive = [NONE | SDAMR | SDAAR]
- ProcessCriticalFailureActionWhenMateFaulty = [NONE | SDAMR | SDAAR]

These parameters allow different types of Automatic Restart shutdowns to be specified when a process encounters a critical fault in Active, Standby, or Mate Faulty. For example, if the NIM (Node Interface Monitor) encounters a critical fault in Active, a FISS could be specified, but if it encounters the fault in Standby, an SDAAR could be specified.

FISS is not an option when the process is in a Standby state or a Mate Faulty state.

Troubleshooting

Note The following troubleshooting procedure can be used any time a platform side goes OOS due to a fault.

Troubleshooting of a platform shutdown can be completed using the Automatic Restart feature saved.debug directory. When a platform shutdown occurs, useful debugging information (cores, logs, and so on) is saved and compressed in a tar file. This file is located in the directory <platform>/bin/saved.debug. To recover the tar file information and to clear the tar file disk space, complete the following steps:

Step 1 Download the time stamped tar file from the saved.debug directory to a system for offline debugging. An example filename is: saved.debug.2007_02_16__16_07_09.tar.Z.

Step 2 Remove the tar file from the disk after it is downloaded to conserve disk space.

Switchover in Progress–Maintenance (101)

The Switchover in Progress alarm (critical) indicates that a system switchover is in progress. This alarm is issued when a system switchover is in progress either due to manual switchover (by a CLI command), failover switchover, or automatic switchover. For additional information, refer to "Maintenance (101)" section on page 7-56.

Side Automatically Restarting Due to Fault–Maintenance (117)

The Side Automatically Restarting Due to Fault alarm (critical) indicates that a platform side is automatically restarting due to a fault condition. This alarm indicates that an Automatic Restart is pending and at what time it will be attempted. For additional information, refer to "Maintenance (117)" section on page 7-64.

Sh Interface Troubleshooting

This section explains how to troubleshoot disaster recovery.

Disaster Recovery

The Diameter Request policy PRIORITY-ORDER means the BTS 10200 always selects the Diameter peer with the highest priority as long as the peer is operational. It prevents switchover if all the peers go down.If the BTS 10200 cannot establish a connection with the highest priority peer, it resends the pending transactions to the peer with the second-highest priority. If the higher priority peer comes back up, the BTS 10200 sends new Diameter requests to the higher priority peer.

During switchover the BTS 10200 does the following:

1. Tears down Diameter connections on the previously-active side.

2. Creates Diameter connections from newly-active side to all Diameter peers IN-SERVICE.
   or
   If peers are unreachable, the BTS 10200 active side does not switchover. Instead it attempts to reestablish the connection with its peers using DIA_REATTEMPT-INTERVAL and DIA_RETRY_COUNT.
   DIA_REATTEMPT-INTERVAL—number of seconds until the DIA_RETRY_COUNT is DIA_RETRY_COUNT
3. The BTS 10200 active side re-attempts to setup the Diameter connection.

CHAPTER 17

Disk Replacement

Revised: August 10, 2011, OL-25016-01

Introduction

This chapter describes the process of replacing a defective Cisco BTS 10200 Softswitch disk. Each Cisco BTS 10200 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
- Perform a full system back up.

The part number of the replacement disk must be the same as the part number of the defective disk, or the size of the replacement disk must be equal to or larger than the mirrored good disk.

This chapter contains the following sections:

System Back Up Procedure

The purpose of this section is to describe the needed steps to create a back up using the Flash Archive on Cisco BTS 10200 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 back up 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 procedure, so that a stable backup is preserved.

Call Agent/Feature Server Back Up

Perform the following steps on the standby CA/FS system:

Step 1 Log in 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, and so on.

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.gz
<hostname># tar -cf - /opt/OptiCall/FSAINxxx/bin/data |gzip -fast - >
/mnt/data.<hostname>.FSAIN.gz
<hostname># tar -cf /opt/OptiCall/FSPTCxxx/bin/data |gzip -fast - >
/mnt/data.<hostname>.FSPTC.gz
```

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/opt/OptiCall/CAxxx/bin/data
<hostname># vi /tmp/excluded_dir/opt/OptiCall/CAxxx/bin/logs
<hostname># vi /tmp/excluded_dir/opt/OptiCall/FSAINxxx/bin/data
<hostname># vi /tmp/excluded_dir/opt/OptiCall/FSAINxxx/bin/logs
<hostname># vi /tmp/excluded_dir/opt/OptiCall/FSPTCxxx/bin/data
<hostname># vi /tmp/excluded_dir/opt/OptiCall/FSPTCxxxx/bin/logs
<hostname># vi /tmp/excluded_dir/opt/Build
```

Note Where **xxx** is the instance number.

Step 10 Back up 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 Switch over 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 Back Up

Perform the following steps on standby EMS/BDMS system:

Step 1 Remove all unnecessary files or directories such as /opt/Build, application **tar** files, and so on.

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>.gz
```

Step 5 Create excluded directories file for flash archive.

```
<hostname># vi /tmp/excluded_dir/data1/oradata
<hostname># vi /tmp/excluded_dir/opt/data/oradata
<hostname># vi /tmp/excluded_dir/opt/Build
```

Step 6 Start all platforms.

```
<hostname># platform start -nocopy
```

Step 7 Verify all platforms are up on standby.

```
<hostname># nodestat
```

Step 8 Back up 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 Unmount NFS server.

```
<hostname># umount /mnt
```

Step 10 Switch over 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 refers to the SCSI controller ID of the system (either 0 or 1). To find out the controller ID, use the **format** command.

Step 1 Log in as root.

Step 2 Verify application status.

```
<hostname>#nodestat
```

Note If all platforms on this node are ACTIVE, then you need to switch over to STANDBY side using the CLI command.

Step 3 Stop all Cisco 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 off line.

```
<hostname>#cfgadm -c unconfigure c1::dsk/cxt0d0
```

Example:

```
Secca38#cfgadm -c unconfigure c1::dsk/c1t0d0
```

Step 10 Verify that Disk 0 is off line.

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   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@0,0 (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 Cisco 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 refers to the SCSI controller ID of the system (either 0 or 1). To find out the controller ID, use the **format** command.

Step 1 Log in as root.

Step 2 Verify application status.

```
<hostname>#nodestat
```

Note If all platforms on this node are ACTIVE, then you need to switch over to STANDBY side using the CLI command.

Step 3 Stop all Cisco 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 off line.

```
<hostname>#cfgadm -c unconfigure c1::dsk/cxt1d0
```

Example:

```
Secca38#cfgadm -c unconfigure c1::dsk/c1t1d0
```

Step 10 Verify that Disk 1 is off line.

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 Cisco BTS 10200 platforms.

```
<hostname>#platform start -nocopy
```

APPENDIX A

Recoverable and Nonrecoverable Error Codes

Revised: August 10, 2011, OL-25016-01

MGCP Normal, Recoverable, and Nonrecoverable Error Codes

This appendix lists normal, recoverable and nonrecoverable error codes for the Cisco BTS 10200 Softswitch. Table A-1 sorts Media Gateway Control Protocol (MGCP) error codes into three categories: normal, recoverable, and nonrecoverable. Table A-1 also provides some of the behavior of the Cisco BTS 10200 for different MGCP message error codes. Endpoint connection（EPCF) and audit connection（AUCX) messages are not sent by the Cisco BTS 10200 to the gateway.

Table A-1 MGCP Normal, Recoverable, and Nonrecoverable Error Codes

MGCP Error Code	Description	AUEP[1]	DLCX[2]	CRCX[3]	MDCX[4]	RQNT[5]
200	The requested transaction was executed normally.	N[6]	N	N	N	N
250	The connection was deleted.	F[7]	N	N	N	R
400	Transient error. If this code is received, the Cisco BTS 10200 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[8]	R	R	R	R
401	Phone is already off-hook. If this code is received, the Cisco BTS 10200 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 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 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 automatically recovers by auditing the endpoint, deleting any available connections and then idling the endpoint.	F	F	N	N	R

Table A-1 MGCP Normal, Recoverable, and Nonrecoverable Error Codes (continued)

MGCP Error Code	Description	AUEP[1]	DLCX[2]	CRCX[3]	MDCX[4]	RQNT[5]
405	The transaction could not be executed, because the endpoint is "restarting."	R	F	N	N	R
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, for example, 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 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 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 (for example, Connection-ID not associated with this Call-ID).	F	N	N	N	R
517	Unsupported or invalid mode.	F	F	F	N	R

Table A-1 MGCP Normal, Recoverable, and Nonrecoverable Error Codes (continued)

MGCP Error Code	Description	AUEP[1]	DLCX[2]	CRCX[3]	MDCX[4]	RQNT[5]
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
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 (for example, 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 (for example, missing, erroneous, unsupported, unknown, and so on).	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

Table A-1 MGCP Normal, Recoverable, and Nonrecoverable Error Codes (continued)

MGCP Error Code	Description	AUEP[1]	DLCX[2]	CRCX[3]	MDCX[4]	RQNT[5]
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
803		F	F	N	F	F
Unknown like 900		F	F	F	F	F
Invalid or absent transaction identifier		RX[9]	RX	RX	RX	RX

1. AUEP—audit endpoint
2. DLCX—delete connection
3. CRCX—create connection
4. MDCX—modify connection
5. RQNT—notification request
6. Normal (N)—Other than 200 error code; the Cisco BTS 10200 clears the call.
7. Faulty (F)—The Cisco BTS 10200 clears the call.
8. Recoverable (R)—The Cisco BTS 10200 clears the call and starts finite recovery or nonrecoverable (NR).
9. For 400 error codes, the Cisco BTS 10200 retransacts (RT) the corresponding MGCP message. The Cisco BTS 10200 also retransmits (RX) the MGCP message with the same transaction.

APPENDIX B

System Usage of MGW Keepalive Parameters, Release 6.0

Revised: August 10, 2011, OL-25016-01

Introduction

This document 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 document 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)
  - term-seize-unreach (default = N)
  - target-disconnect-timer (default = 60 seconds)

Note The default value of target-disconnect-timer is 60 seconds for fresh installations of Release 6.0 software. For systems being upgraded to Release 6.0, the default is 20 seconds. For details, see the "MGCP-MAX2-RETRIES, MGCP-T-MAX and TARGET-DISCONNECT-TIMER" section on page B-8.

  - keepalive-fail-release-timer (default = 36,000 seconds)

- In the call-agent table:
  - mgw-monitoring-enabled (default=Y)
- In the ca-config table:
  - mgcp-t-max (default = 20 seconds)
  - mgcp-t-hist (default = 30 seconds)
  - mgcp-rto-max (default = 4 seconds)
  - mgcp-high-and-wet-interval (default = 5 minutes)
  - mgcp-high-and-wet-retries (default = 3)
  - mgcp-high-and-dry-interval (default = 60 minutes)
  - mgcp-max-keepalive-auep (default = 20,000)

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.

- Controlling the impact of unreachable status—If you set **term-seize-unreach** to Y, the BTS 10200 attempts to set up calls to the MGW even if it has declared the MGW unreachable. This is useful if the MGW is able to receive calls, but the BTS 10200 is not scheduled to send an AUEP message to the MGW for several more minutes or hours. If you leave **term-seize-unreach** at its default value of N, the BTS 10200 does *not* attempt to set up calls if it has declared the MGW unreachable.

Caution For mgw-profile tables applicable to TGWs, Cisco strongly recommends leaving the term-seize-unreach parameter at its default value (N) if you have included multiple TGWs in a single trunk group. Otherwise, the BTS 10200 might repeatedly attempt to route calls to an unreachable TGW, even when reachable TGWs are available in the same trunk group.

- 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**.

Tip The **status mgw** command can display the status of a MGW as **working status** or **down status**; the **status mgw_tab** command can display the status of a MGW as **REACHABLE** or **UNREACHABLE**. Working status is equivalent to REACHABLE, and down status is equivalent to UNREACHABLE.

- KA attempt (AUEP transaction)—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. The KA attempt is defined as failed if no ACK is received after the defined number of AUEP retransmissions and within a defined waiting period (**target-disconnect-timer**).
- 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 Cisco BTS 10200 Softswitch CLI Database.

- 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 a MGW.
- **mgcp-max-keepalive-auep** (default = 20,000)—This field specifies maximum number of MGWs to be AUEP pinged in any 10 second interval.

Querying Status of MGWs and Subscribers With Tabular Display

You can use the following commands to run queries for unreachable MGWs, or unreachable subscriber terminations. The system provides a tabular display of the status for MGWs or subscribers.

All Records with oper_state=UNREACHABLE

```
status mgw_tab oper_state=UNREACHABLE;
```

For this command:

- For the oper_state, you can enter REACHABLE, UNREACHABLE, or UNKNOWN to define your query.
- A maximum of 1,000 records can be displayed at one time.

Limited Range of Records with oper_state=UNREACHABLE

```
status mgw_tab oper_state=UNREACHABLE; limit=1000; start_row=0;
```

For this command:

- You can specify the maximum number of rows to display (limit) and the first row that you want displayed (start_row).
- Set the maximum number of records that you want to be displayed (limit) to any number 0–1,000.
- The start_row value can be set to 0–N, where N is the maximum number of records generated by the query.

Unreachable Subscribers

Use the following command to query an unreachable subscriber.

```
status subscriber_termination_tab oper_state=UNREACH; limit=1000; start_row=0;

status subscriber_termination_tab call_state=BUSY; limit=1000; start_row=0;
```

For this command:

- You must enter either the oper_state or the call_state. You cannot enter both.
- For the oper_state, you can enter UNKNOWN, ACTIVE, MTRANS, DOWN, FAULTY, UNREACH, or OFF_NORMAL to define your query. OFF_NORMAL is the equivalent of UNREACH, FAULTY, or DOWN.
- For the gateway call_state you can enter IDLE, BUSY, CTRANS_BUSY.

- Narrow the command with the limit parameter if the results are greater than 1,000 records, which is the maximum number of records the system can display at one time.
- The start_row value can be set to 0–N, where N is the maximum number of records that exist as a result of the query.

Output to File

You can send the output of these commands to a file, and there is no restriction on the number of records that can be sent. You do this by adding **output=<filename>; output_type=xxx** to the command, where xxx can be CSV or XML. CSV = comma-separated values. The following are examples.

```
status mgw_tab oper_state=UNREACHABLE; limit=1000; start_row=0; output=<filename>;
output_type=CSV;

status subscriber_termination_tab call_state=BUSY; limit=1000; start_row=0;
output=<filename>; output_type=CSV;
```

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.

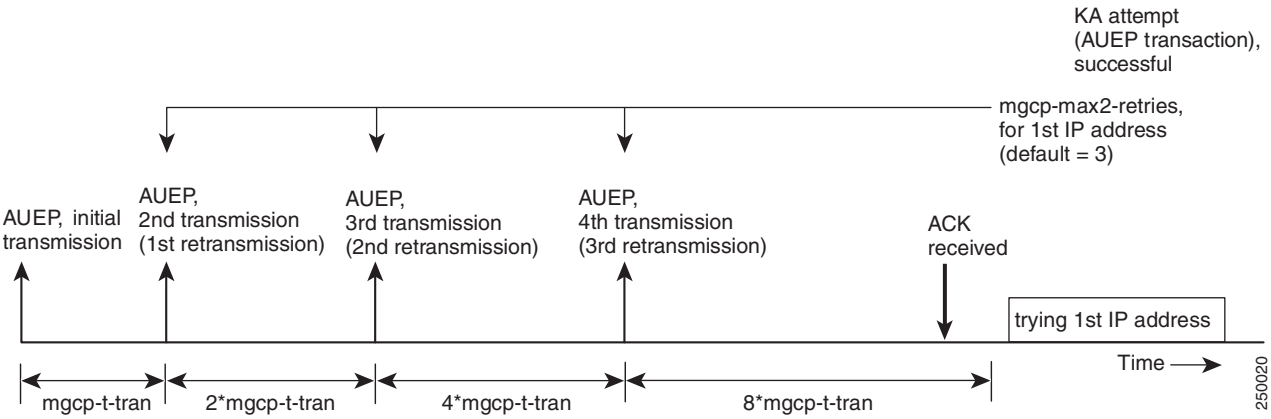
In a typical network, the average response time is much less than 400 milliseconds. Therefore, in this section, the drawings show the initial waiting period as **mgcp-t-tran**.

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

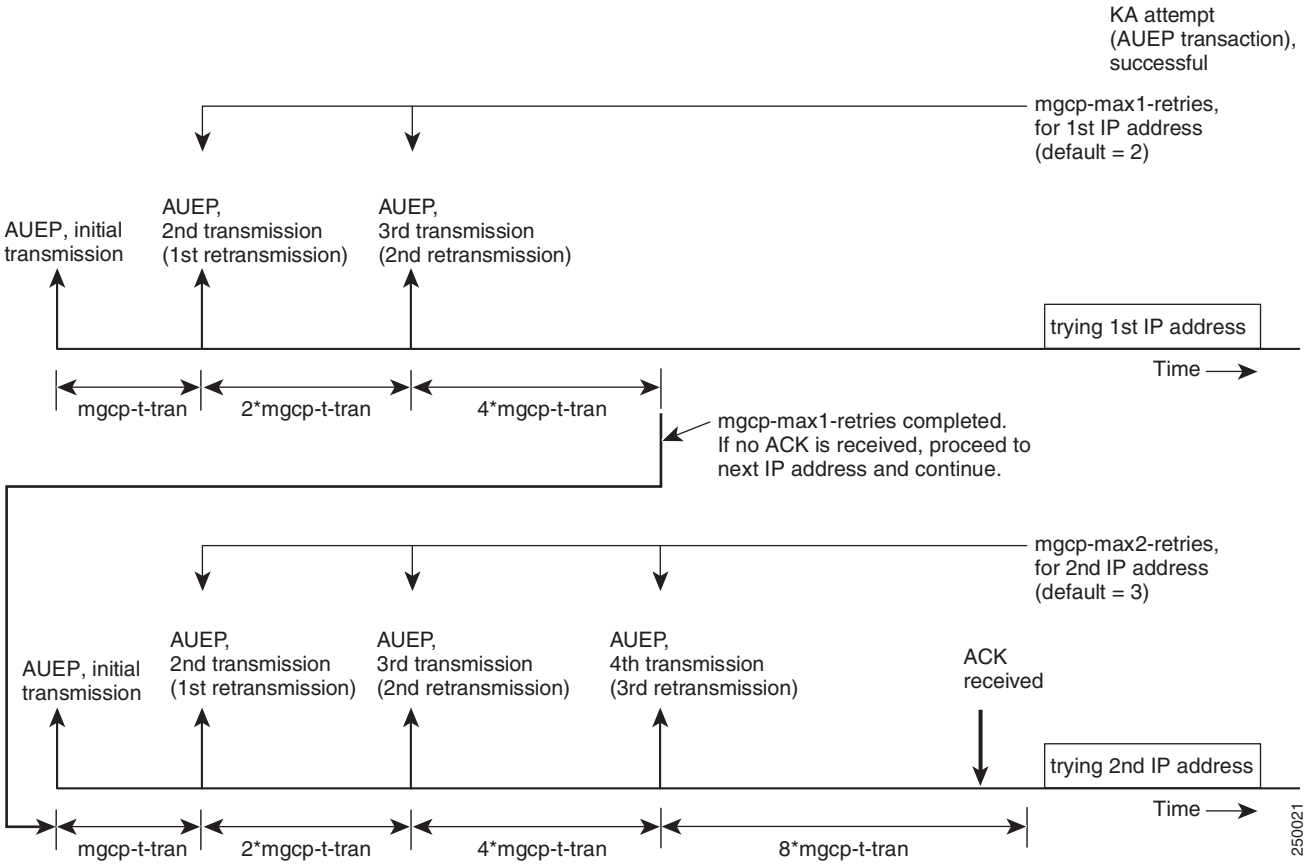


Note for Figure B-1

See the additional information about **mgcp-t-tran** in the "Initial Transmission Waiting Period (mgcp-t-tran)" section on page B-5.

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 for Figure B-2

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

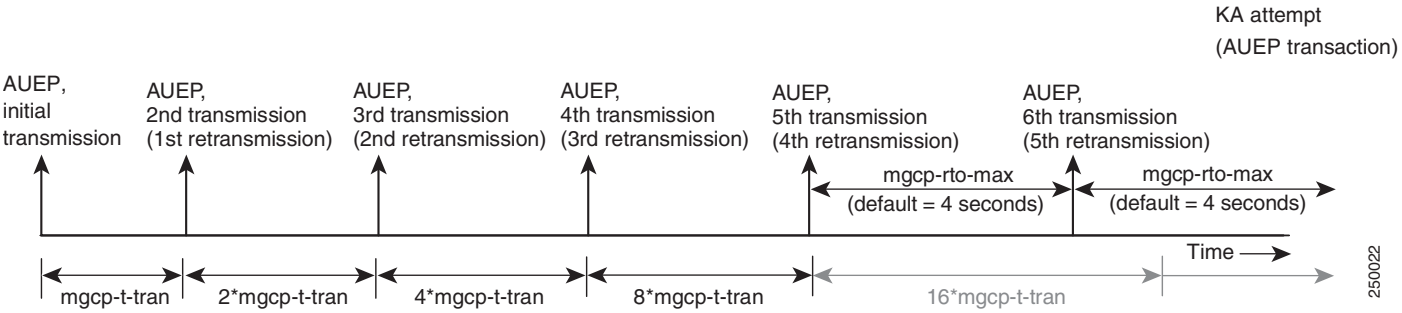
This section explains how the system handles MGCP message retransmissions and takes action when no ACK is received from the MGW.

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 for Figure B-3

See the additional information about **mgcp-t-tran** in the "Initial Transmission Waiting Period (mgcp-t-tran)" section on page B-5.

MGCP-MAX2-RETRIES, MGCP-T-MAX and TARGET-DISCONNECT-TIMER

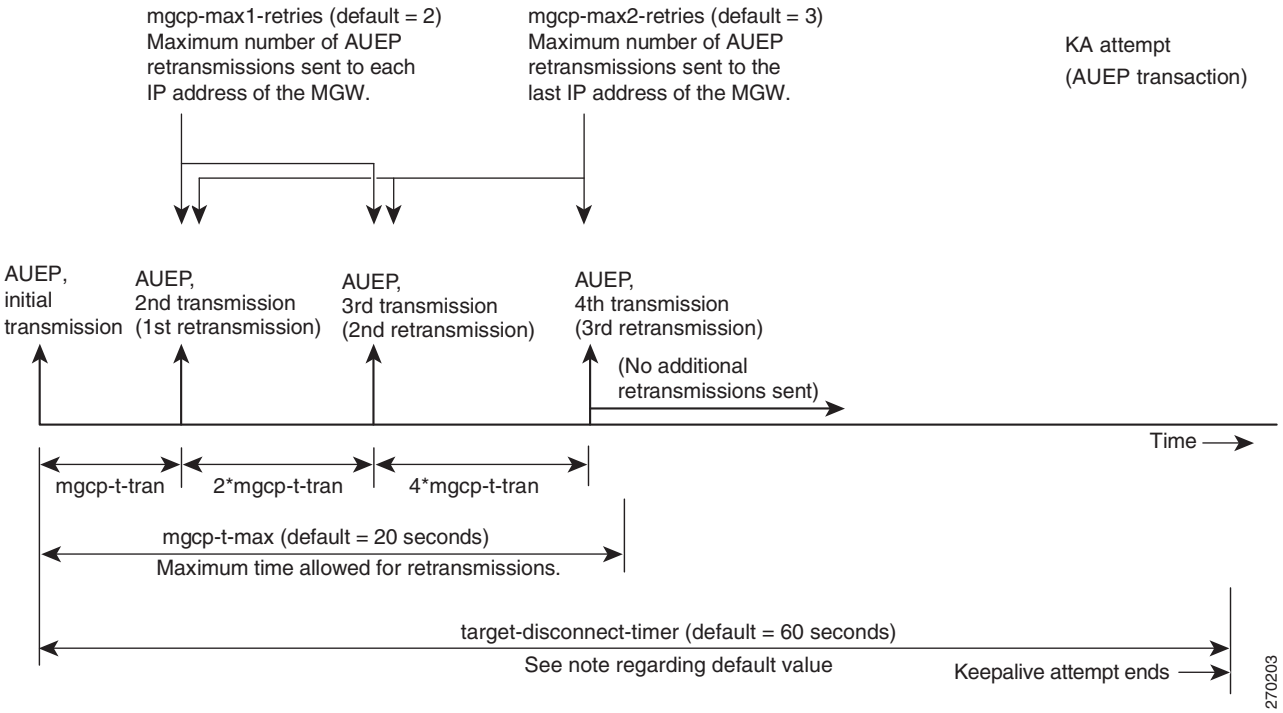
The BTS 10200 limits retransmissions of the AUEP message to **mgcp-max2-retries** or a total duration of **mgcp-t-max** (default = 20 seconds), whichever occurs first.

If the BTS 10200 does not receive an ACK response from the MGW before the expiration of **target-disconnect-timer** (default value 60 seconds), the BTS 10200 abandons the transaction and takes *one* of the following additional actions:

- 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-10) 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 UNREACH.
- If keepalive functionality is *disabled* on the system, there will be no expedited keepalive process, and the system marks the operational status of the affected terminations as UNREACH.

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. The system waits for an ACK until the target-disconnect-timer expires. When that timer expires, the KA attempt ends.

Figure B-4 AUEP Retransmissions and No ACK Received



Note for Figure B-4

For fresh installations of Release 6.0 software, the default value for **target-disconnect-timer** is 60 seconds, as shown in Figure B-4. However, if you have upgraded to Release 6.0 from a previous release, the default value was automatically set to 20 seconds during the upgrade process. If you have upgraded, and you previously customized your keepalive interval, you can adjust the value of **target-disconnect-timer** as needed to obtain the desired keepalive interval.

Keepalive Process

This section describes the keepalive (KA) process. The Cisco BTS 10200 performs KA attempts after periods of inactivity to determine whether the status of a MGW should be considered working or down. (A period of inactivity means a time period in which no MGCP message of any kind is received from the MGW.)

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).

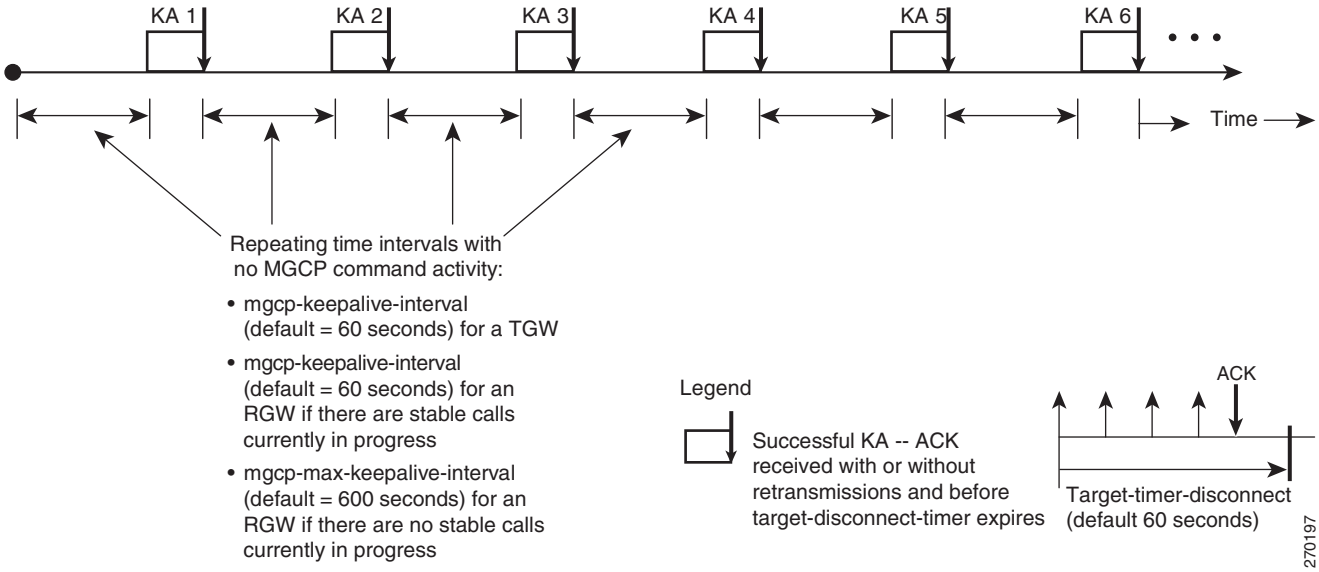
The following scenarios are covered in this section:

Scenario 1—MGW Reachable

This scenario is shown in Figure B-5. The MGW is reachable (an ACK was received during a previous KA attempt), 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). The BTS 10200 starts a new KA attempt.

Note The legend in this drawing explains how successful keepalive attempts are illustrated throughout this document.

Figure B-5 KA Attempts—MGW Reachable



Notes for Figure B-5

See the note regarding the default value of **target-disconnect-timer** below Figure B-4.

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:

- For an RGW—If KA attempts are successful, and stable calls exist, the system continues this pattern of KA attempts. If all the stable calls are finished and there are no more stable calls on the RGW, the system *changes* the waiting period between KA attempts from **mgcp-keepalive-interval** to **mgcp-max-keepalive-interval** (default = 600 seconds).
- For a TGW—If KA attempts are successful, the system continues this pattern of KA attempts, regardless of whether there are stable calls on the TGW.
- If a KA attempt is unsuccessful, the system changes the KA pattern to that shown in Scenario 2—MGW Unreachable.

Scenario 2—MGW Unreachable

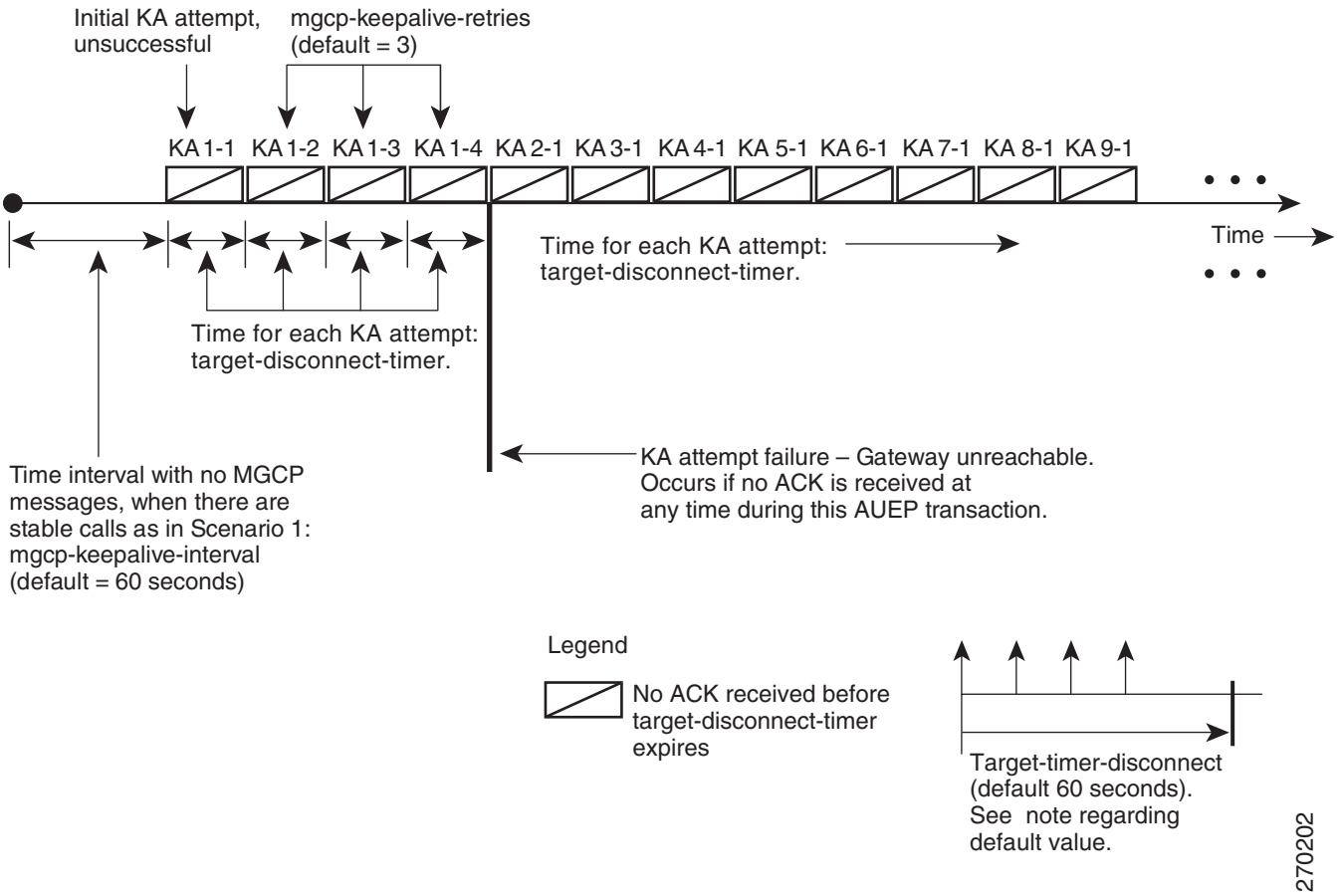
In this scenario, the BTS 10200 performs KA attempts but does not receive an ACK response from the MGW. After the BTS 10200 attempts the number of KA retries provisioned for the parameter **mgcp-keepalive-retries**, it declares the MGW to be unreachable. The BTS 10200 continues to perform KA attempts; the pattern of KA attempts differs between TGWs and RGWs as described in this section.

KA Retries for TGW

The system continues to repeat closely-spaced KA attempts to the TGW, even after the number of attempts exceeds **mgcp-keepalive-retries**. This is shown in Figure B-6.

Note The legend in this drawing explains how unsuccessful keepalive attempts are illustrated throughout this document.

Figure B-6 KA Attempts—TGW Unreachable



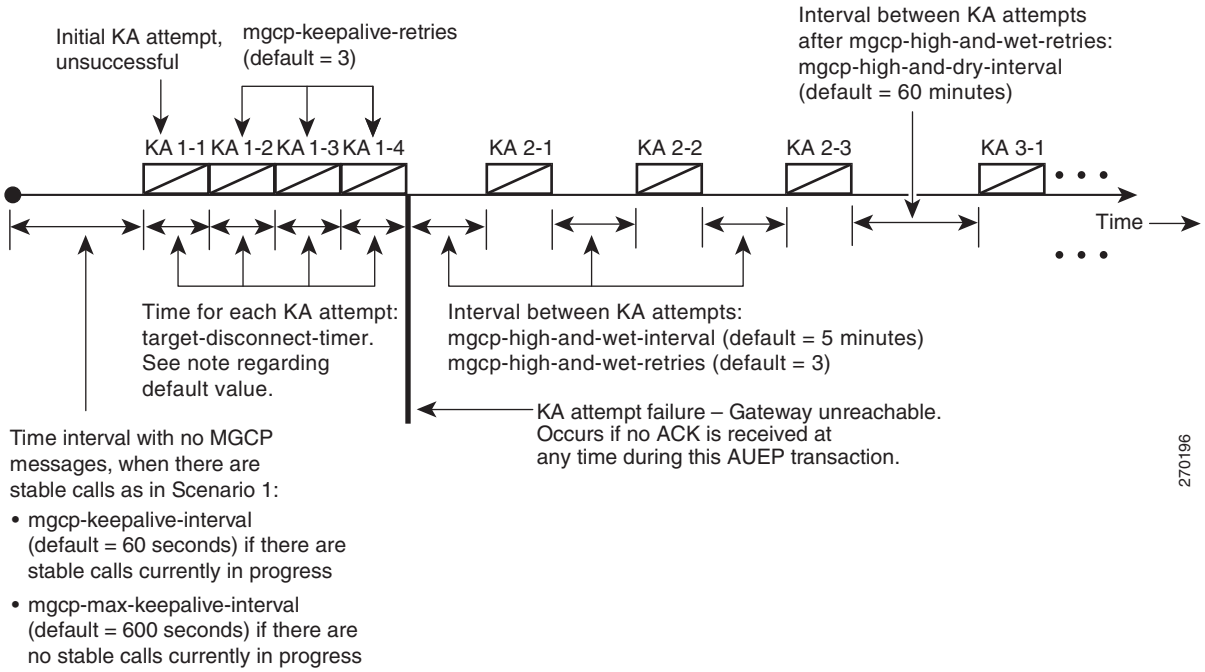
Note for Figure B-6

See the note regarding the default value of **target-disconnect-timer** below Figure B-4.

KA Retries for RGW

The system continues to repeat KA attempts to the RGW. After the number of attempts exceeds **mgcp-keepalive-retries**, the system waits for a provisioned amount of time between successive attempts. This is shown in Figure B-7.

Figure B-7 KA Attempts—RGW Unreachable



Note for Figure B-7

See the note regarding the default value of **target-disconnect-timer** below Figure B-4.

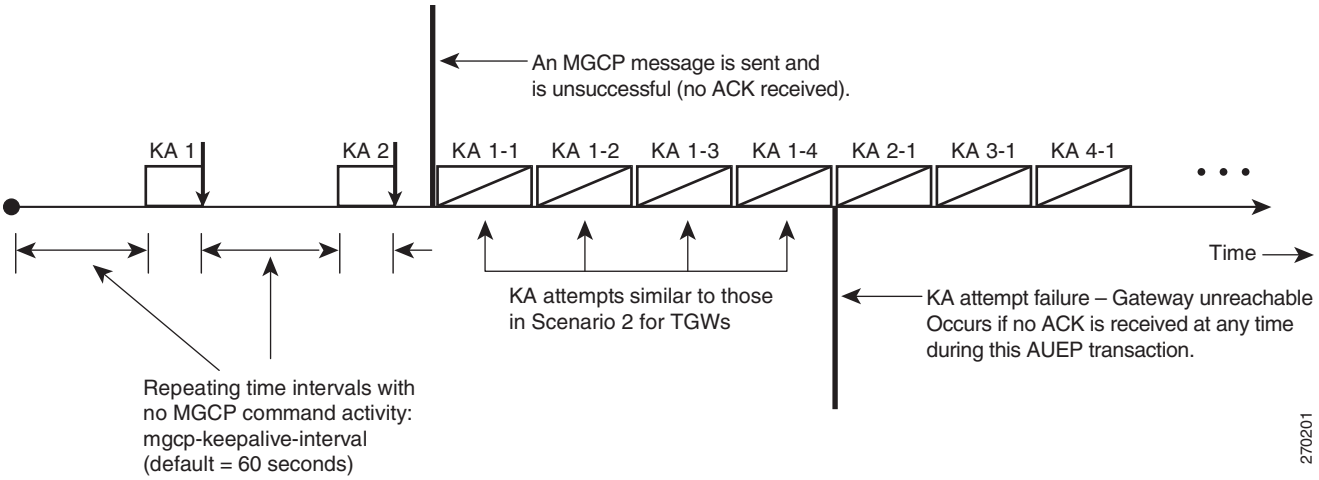
Scenario 3—MGW Previously Reachable but MGCP Message Fails

In this scenario. the MGW was previously reachable (an ACK was received during a previous KA attempt). However, when the BTS 10200 sends an MGCP message to the MGW, the message fails; that is, the BTS 10200 does not receive a reply from the MGW within the allowed timeout period. Subsequent KA attempts fail. The pattern of KA attempts following the failed MGCP message differs between TGWs and RGWs as described below.

KA Retries for TGW

The system performs KA attempts to the TGW as shown in Figure B-8.

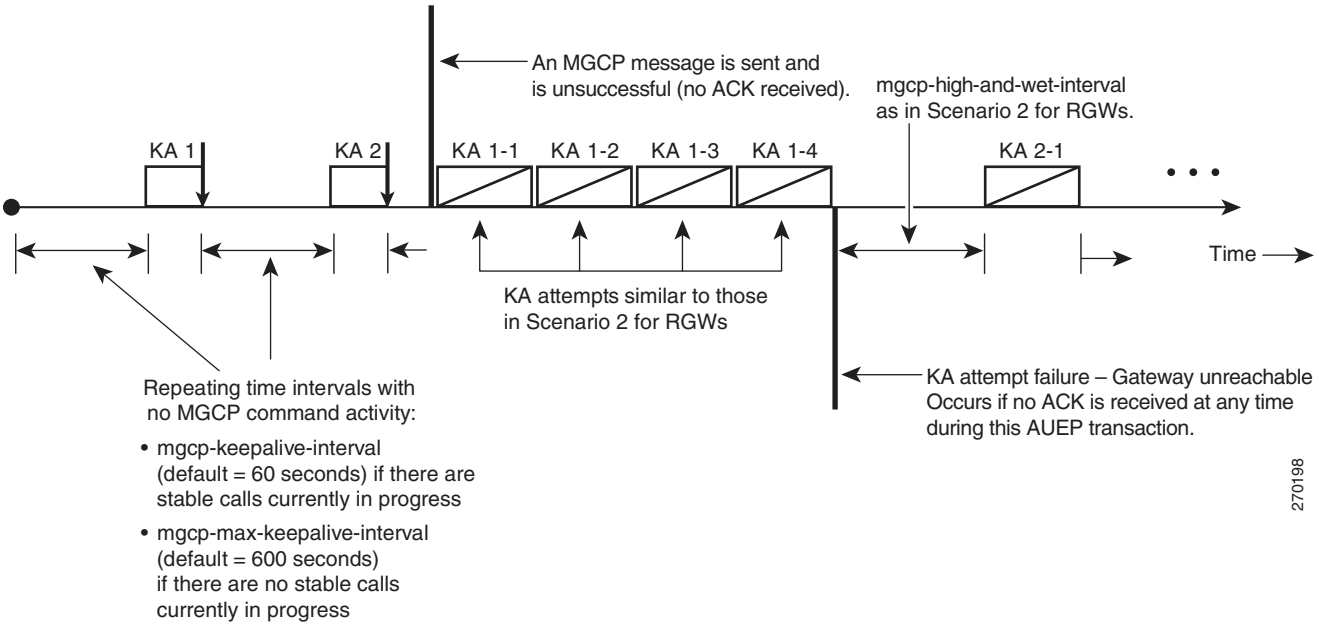
Figure B-8 KA Attempts—TGW Previously Reachable but MGCP Message Fails



KA Retries for RGW

The system performs KA attempts to the RGW as shown in Figure B-9.

Figure B-9 KA Attempts—RGW Previously Reachable but MGCP Message Fails



Scenario 4—MGW Previously Unreachable but MGCP Message Succeeds

In this scenario. the MGW was previously unreachable (an ACK was not received during previous KA attempts). However, the BTS 10200 receives an MGCP message in one of the following manners:

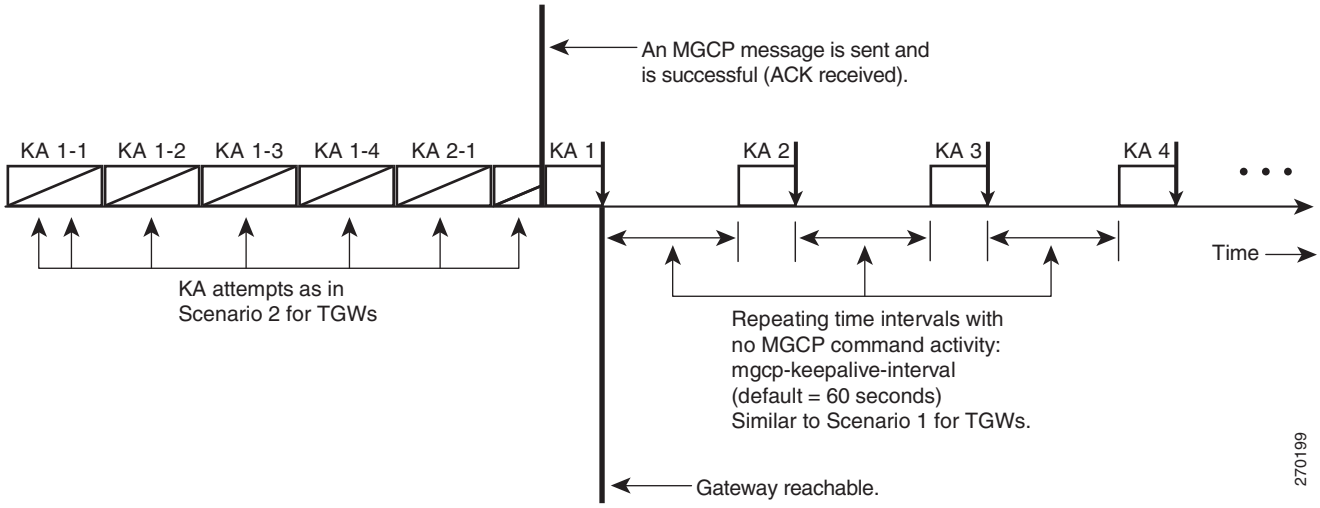
- The BTS 10200 receives a valid MGCP message from the remote MGW.
- The BTS 10200 sends an MGCP message to the MGW and the message succeeds; that is, the BTS 10200 receives a reply from the MGW within the allowed timeout period.

Subsequent KA attempts succeed, and the system declares the MGW to be reachable. The pattern of KA attempts following the failed MGCP message differs between TGWs and RGWs as described below.

KA Retries for TGW

The system performs KA attempts to the TGW as shown in Figure B-10.

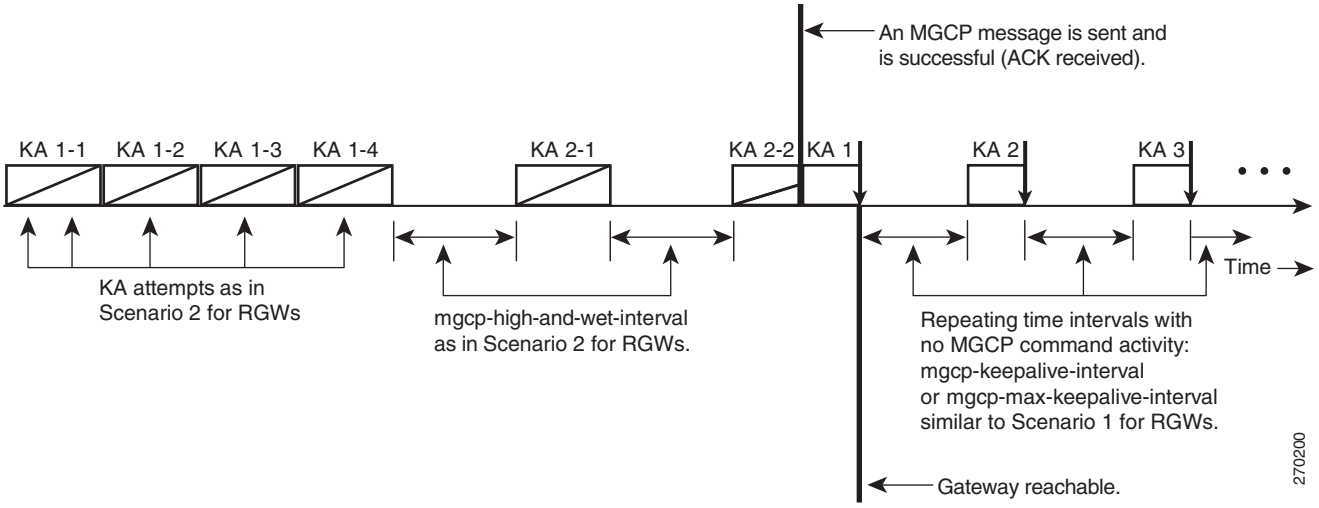
Figure B-10 KA Attempts—TGW Previously Unreachable but MGCP Message Succeeds



KA Retries for RGW

The system performs KA attempts to the RGW as shown in Figure B-11.

Figure B-11 KA Attempts—RGW Previously Unreachable but MGCP Message Succeeds



Note for Figure B-11

For detailed examples of successful KA attempts, see Figure B-1 and Figure B-2.

Events and Alarms Related to the KA Process

Typical alarms for the KA process include:

- SIGNALING (36)—Trunk locally blocked (applicable to CAS, ISDN, and SS7 trunks).
- SIGNALING (79)—Trunking Gateway unreachable.
- SIGNALING (171)—Residential Gateway unreachable.

Typical informational events for the KA process 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.

You can check the status of a MGW or subscriber termination with the status commands listed in the "Managing External Resources" chapter in the *Cisco BTS 10200 Softswitch Operations and Maintenance Guide*, or with the tabular status commands listed in the "Querying Status of MGWs and Subscribers With Tabular Display" section on page B-4. To query events and alarms, see the "Managing Events and Alarms" section in the *Cisco BTS 10200 Softswitch Troubleshooting Guide*.

APPENDIX C

Overload Control

Revised: August 10, 2011, OL-25016-01

Overload Control Processes

Overload is a switch condition that exists when system resources cannot handle system tasks. Increases in call traffic or messages indirectly related to call traffic usually cause overload. The overload control processes are listed in Table C-1.

The Overload Control feature supports the Cisco BTS 10200 Softswitch Call Agent (CA) and Feature Server (FS). Overload Control detects, controls, and manages overload from all types of networks (SIP, SS7, ISDN, MGCP, H.323).

Table C-1 Overload Control Processes

Overload Control Phase	Actions
1. Automatic detection and handling	Measures and compares factors to threshold values. Determines system congestion and machine congestion level (MCL). Detects Cisco BTS 10200 machine congestion conditions in 5 levels: none, mild, moderate, severe, emergency. Automatically reduces overload as described.
2. Reporting	Affects the following switch areas: • Alarms • Logs • Billing • Measurements

Note The monitoring of the CPU load of critical processes is *not* supported.

Detecting Overload

In the detection phase of Overload Control, any one of three factors can have the highest MCL. This value dictates the MCL for the entire system. The three factors are

- Critical process queue lengths—The olm.cfg configuration file has critical queue lengths for Cisco BTS 10200 processes like BCM, MGA, SGA, SIA, ISA, and H3A. You can define multiple (32 factors total) critical queues for any Cisco BTS 10200 process. The Cisco BTS 10200 monitors the usage proportion of each critical IPC queue.
- IPC buffer pool usage—Cisco BTS 10200 monitors the proportion of available buffers in the IPC buffers pool. This reflects MCL: the higher the usage, the greater the congestion.

Cisco BTS 10200 detects its own MCL in five levels:

- MCL0—No congestion and no need for any abatement.
- MCL1—Mild congestion. Call rejection starts as configured in olm.cfg.
- MCL2—Moderate congestion. Call rejection increases as configured in olm.cfg.
- MCL3—Severe congestion. Call rejection increases still more as configured in olm.cfg.
- MCL4—Emergency congestion. Cisco BTS 10200 rejects all calls including emergency calls.

Computing MCL

The Cisco BTS 10200 computes factor levels by calculating averages for each factor. The rate of sampling (number of slots) can be configured per factor (3–10 slots). The MCL is set according to a factor level. In Table C-2 thresholds are set to 50, 70, 90, and 95 percent.

Table C-2 MCL Thresholds

Onset /abatement thresholds	Factor Level	MCL
—	0–49	MC0
level_1_threshold = 50	50–69	MC1
level_2_threshold = 70	70–89	MC2
level_3_threshold = 90	90–94	MC3
level_4_threshold = 95	95–100	MC4

Reducing Overload

When MCL exceeds MCL0, overload control reduces MCL as follows:

- Selectively reject new calls by the signaling adapters—A percentage of calls and messages are rejected at the current MCL level, based on olm.cfg. Emergency calls are not rejected at MCL 1–3, but all calls, including emergency calls, are rejected at MCL4.
- Tell the network to stop sending traffic—This starts when the Cisco BTS 10200 is mildly congested (at MCL1) and continues through all higher MCL levels until the overload condition abates to MC0. This action can only be applied to the following types of networks:
  - SS7 sends Automatic Control Level (ACL) parameter in ISUP release messages.
  - H.323 sends Resource Availability Indicator (RAI) message.
  - SIP sends 500 or 503 with a retry.
- CA stops sending triggers to POTS FS—When the FS is congested the following occurs:
  - FS notifies CA once of its congested status.
  - CA sends only emergency triggers to FS, as it manages FS's congestion abatement.

Slowing Overload Reduction

Sudden abatement reduction might cause MCL to rapidly increase again. To counteract MCL "bouncing," MCL reduces one MCL level at a time, regardless of how low computed MCL becomes. This permits the system MCL to reduce gracefully over a number of intervals.

Overload Implementation and Configuration

This section discussed the following items:

- Configuring Emergency Call Handling
- Signal Adapter Call Rejection
- Configuring the SIP Response Code
- SIP Message Handling
- H.323 Message Handling
- SS7 Automatic Control Parameter

Note These tasks include examples of CLI commands that illustrate how to provision the specific feature. For a complete list of all CLI tables and tokens, refer to the Cisco BTS 10200 Softswitch CLI Database.

Configuring Emergency Call Handling

The Cisco BTS 10200 checks the

- Called-party number for all incoming calls against the EMERGENCY-NUMBER-LIST
- Calling party category (CPC) in ISUP calls

If the Cisco BTS 10200 determines it is an emergency call and the MCL is 1, 2, or 3, the Cisco BTS 10200 gives it priority and does not reject the call. If the MCL is 4, The Cisco BTS 10200 rejects all calls, including emergency calls.

To add a number to the EMERGENCY-NUMBER-LIST, enter a command similar to the following:

```
add emergency-number-list digit_string=911;

Reply: Success: at 2006-02-28 09:48:40 by btsadmin
MNT add successful
Transaction 934823299797597704 was processed.
```

To display the EMERGENCY-NUMBER-LIST, enter:

```
show emergency-number-list;

DIGIT_STRING=911

Reply: Success: at 2006-02-28 09:48:45 by btsadmin
Entry 1 of 1 returned.
```

To delete a number from the EMERGENCY-NUMBER-LIST, enter a command similar to the following:

```
delete emergency-number-list digit_string=911;

Reply: Success: at 2006-02-28 09:52:20 by btsadmin
MNT delete successful
Transaction 934823480106794504 was processed.
```

Signal Adapter Call Rejection

The OLM process provides functionality by which adapters can call to see if a particular call or event should be rejected. This functionality determines whether a call or message should be accepted or rejected. The calling signaling adapter provides a message/call number (or allow a default value to be used by OLM), and the percentage of calls/messages to be rejected at the current MCL level (or allow a default value to be used by OLM).

The first parameter is an integer containing the message/call number value to be used for the call rejection calculation.

The second parameter is an integer containing the percentage of calls to be rejected.

The third parameter can be set to either OLM_API_CALL_TYPE_ORDINARY or OLM_API_CALL_TYPE_EMERGENCY. When set to OLM_API_CALL_TYPE_ORDINARY, the function always returns FALSE if the system MCL is at level 4. When set to OLM_API_CALL_TYPE_EMERGENCY, the function always returns true ignoring the other parameters unless the system MCL is at level 4 in which case it again returns false. Per the selection of parameter 4, emergency calls are not normally subject to any rejection at MCL 0 – 3, but all calls including emergency calls are rejected at MCL4.

Based on these parameters, the function then returns either false - do not accept the message/call/session, or true - accept the message/call/session. In the case of MCL4, the function always returns false.

SS7 (SGA) Implementation of Call Rejection

An SS7 (SGA) implementation provides defaults for the first two parameters, so OLM provides both the random seed for the percentage of rejections and the actual reject rates. In addition, the called-party number for all incoming calls is checked against the EMERGENCY-NUMBER-LIST table to determine whether the call is an emergency call. Also in ISUP implementations, the calling party category is checked to see if it is an emergency line. If the incoming call is an emergency call (that is, called-party number is found in the table or CPC is emergency), it is given priority and not rejected outright in case of MC1, 2, and 3. In case of MC4, all calls are to be rejected.

H323 Implementation of Call Rejection

For an H.323 implementation, the default behavior is to used for OLM reject percentage values (H.323 calls with OLM_API_USE_DEFAULT_PERCENTAGE). However, H.323 also provides the option to use command-line arguments to over-ride the default OLM percent values. In that case, H.323 passes the value. For the message number, H.323 always uses OLM_API_USE_DEFAULT_MSG_NUM.

SIA (SIP) Implementation of Call Rejection

An SIA (SIP) implementation provides the actual message number and the rejection percentage. This is because SIP not only deals with calls (invites), but with other messages such as register, subscribe, notify, and options messages. The messages may or may not have any call context.

ISA Implementation of Call Rejection

An ISA implementation provides defaults for the first two parameters, so OLM provides a random number for the percentage of rejections and the actual reject rates. In addition, the called-party number for all incoming calls is checked against the EMERGENCY-NUMBER-LIST table to determine whether the call is an emergency call. If the incoming call is an emergency call (that is, called-party number is found in the table), it is given priority and not rejected outright in case of MC1, 2, and 3. In case of MC4, all calls are to be rejected.

Configuring the SIP Response Code

When rejecting a SIP message during overload, the Cisco BTS 10200 can use either of the following:

- 500 Server Internal Error
- 503 Service Unavailable

Use the following command. The default value is 503.

```
add ca_config type=SIA-OC-REJECTION-RESP; datatype=integer; value=500;
```

SIP Message Handling

When processing an incoming SIP call, the Cisco BTS 10200 looks at the MCL of the CA. It uses the following factors to decide whether to accept or reject the message:

- SIP Message Type
- Call type (normal or emergency)
- Configured rejection percentage
- Current MCL status

SIP Message Types

This section provides information on the SIP message types.

Message Rejection: Invite

If it is overloaded, the Cisco BTS 10200 rejects a percentage of incoming invite messages. The percentage rejected is based on sia.cfg. Only new invite messages are checked for acceptance. Reinvite messages are always accepted.

Message Rejection: Register

If it is overloaded, the Cisco BTS 10200 rejects a configured percentage of register messages.

Message Rejection: Refer

If it is overloaded, the Cisco BTS 10200 rejects a a percentage of incoming refer messages.

Message Rejection: Subscribe

If it is overloaded, the Cisco BTS 10200 rejects a configured percentage of out-of-dialog subscribe messages. The Cisco BTS 10200 also rejects subscribe messages without call contexts. The Cisco BTS 10200 does not reject subscribe messages received in an invite dialog.

Message Rejection: Options

If it is overloaded, the Cisco BTS 10200 rejects options messages. There is no configuration required; all options messages are rejected between MCL1 and MCL4.

Message: Unsolicited Notify Repression

If it is overloaded, the Cisco BTS 10200 does not send unsolicited notify messages (MWI requests) to endpoints. However, even if it is overloaded, the Cisco BTS 10200 receives and processes unsolicited notify requests.

UDP Messages

The Cisco BTS 10200 drops messages like stun if they are less than the configured size. This applies to UDP messages.

Message Rejection Logic

When the Cisco BTS 10200 rejects an incoming SIP call it responds with 500 or 503. Use the CLI to set the response code.

The Cisco BTS 10200 includes a Retry-After header in its response. The value (in seconds) in this header notifies the endpoint that the Cisco BTS 10200 does not receive further requests for the specified time. For example, “Retry-After: 5” means the endpoint should send the next request to the Cisco BTS 10200 only after 5 seconds has passed.

H.323 Message Handling

This section provides information on the H.323 message handing.

Call Rejection—System MCL

When a complete H.225 setup message is received, an application-provided call-back function is used to check whether the call should be rejected immediately or accepted based on the MCL state. The OLM determines whether the call should be rejected based on its default call reject percentages and the system-MCL. The H.323 process checks whether the call is an emergency call before releasing it. If it’s an emergency call, it is accepted.

Call Rejection—IPC Queue

For incoming TCP-based calls, the H.323 process checks the IPC queue for congestion. If the queue is congested, the H.323 process responds to all valid setup message with an H.225 ReleaseComplete with a CauseCode=42, and CallCapacity information with CallsAvailable=0, to indicate congestion. The TCP connection is released immediately.

The H.323 process checks whether the call is an emergency call before releasing it. If it's an emergency call, it attempts one more time to post the call to the worker thread.

Congestion on Peer Gateway

A terminating peer H.323 Gateway (or IP-IP Gateway) can indicate congestion by sending a ReleaseComplete with CauseCode=42 or with CallCapacity data with CallsAvailable=0. If either of these two indications is received at the Cisco BTS 10200, the H.323 process sets the acl_set field in the TRUNK-GRP table associated with the H.323 gateway and starts a timer. The timer length is read from the PEER-GW-OVERLOAD-TIMER field of the H323-TG-PROFILE table configured for the TRUNK-GRP. For the length of the timer, BCM checks and attempts to route calls to an alternate destination.

Reporting Call Capacity

For every incoming call, the H.323 process reports call capacity information to the gatekeeper in the ARQ and DRQ messages and to peer H.323 gateways in the release complete message. In addition, the H.323 process reports call capacity information to the gatekeeper in the RRQ and RAI messages.

Each H.323 instance reports the call capacity as it relates to its available resources. The maximum call capacity is calculated based on the smaller of the provisioned MAX-VOIP-CALLS or the number of available shared memory call-data blocks for the Cisco BTS 10200 H.323 gateway. The current call capacity is the current number of active calls on the H.323 gateway.

Report Alternate Endpoints

The Cisco BTS 10200 virtual H.323 gateway includes provisioned alternate endpoint data. The alternate endpoint data is provisioned through the CLI in the H323-GW table and consists of a TSAP address for each endpoint. The H.323 process is updated by a database trigger whenever this table is changed. Additionally, a full-weight RRQ message including the updated alternate endpoint information is sent to the gatekeeper when the H323-GW table is changed.

Sending RAI to Gatekeeper

A resource availability indicator (RAI) message is sent to the gatekeeper when there is system-wide or H.323 IPC thread congestion. The sending of the RAI message is triggered when there is a system MCL or IPC queue MCL state change.

When a system moves from a noncongested to a congested state, an RAI message is sent with the almost out of resources parameter set to true. When a system transitions from a congested to no-congested state, an RAI message is sent with the almost out of resources parameter set to false. Additionally, the call capacity information is included in the RAI message.

SS7 Automatic Control Parameter

If the current Machine Congestion Level (MCL) is greater than MC0, the Cisco BTS 10200 system includes an automatic congestion level (ACL) parameter in every ISUP release message it sends to linked switches. Receiving the ACL induces the linked switches to reduce the call traffic offered to the system.

Some switches understand up to three levels of congestion indication. Others only understand two. Some ignore the ACL altogether depending on the ISUP variant. The attribute MAX ACL indicates the mapping of the current MCL to the ACL value in the release message, as stated in Table C-3.

Table C-3 MCL to ACL Mapping

MAX ACL	Current MCL	ACL Value in Release Message
0	0, 1, 2, 3, 4	Not Present
2	0	Not Present
	1	1
	2	2
	3	2
	4	2
3	0	Not Present
	1	1
	2	2
	3	3
	4	3

The MAX_ACL value is hard coded in MDL per variant. For example, if a particular ISUP supports a maximum ACL value of 2, then at run time if the current MCL is 3, then according to Table C-3, an ACL value of 2 is sent in all the release messages to this switch.

The SS7 (SGA) process monitors the MCL and includes the ACL in the release messages whenever the MCL is greater than MC0.

Operating

This section explains how to perform the following tasks:

- Viewing MCL
- Measurements

It also explains how this feature affects the measurements operational area.

Viewing MCL

To display the MCL, enter a command similar to the following:

```
status machine-congestion-level platform_id=CA146;

MACHINE CONGESTION LEVEL ON CALL AGENT CA146 IS... ->

ADMIN MCL -> NO_CONGESTION(0)
COMPUTED MCL -> NO_CONGESTION(0)
EFFECTIVE MCL -> NO_CONGESTION(0)
FEATURE SERVER CONGESTION ->
FSAIN205 IS NOT CONGESTED
FSPTC235 IS NOT CONGESTED
REASON -> ADM executed successfully
RESULT -> ADM configure result in success

Reply : Success: at 2006-02-28 09:54:27 by btsadmin
```

If platform_id is the FS, for example, FSPTC235, the output shows MCL. If platform_id is the CA, for example, CA146, the output includes congestion status of FSs as seen by the CA. Without this parameter the command displays the MCL of all platforms on the system.

Setting the Minimum System MCL

Warning **Manually setting minimum MCL means call processing is affected exactly as it would be if MCL were set at that level due to actual system overload/congestion. Use it for test purposes only.**

To set the minimum system MCL, enter a command similar to the following:

```
control machine-congestion-level platform_id=CA146, mcl=2;

MACHINE CONGESTION LEVEL ON CALL AGENT CA146 IS... ->

ADMIN MCL -> NO_CONGESTION(0)
COMPUTED MCL -> NO_CONGESTION(0)
EFFECTIVE MCL -> NO_CONGESTION(0)
FEATURE SERVER CONGESTION ->
FSAIN205 IS NOT CONGESTED
FSPTC235 IS NOT CONGESTED
REASON -> ADM executed successfully
RESULT -> ADM configure result in success

Reply: Success: at 2006-02-28 09:54:27 by btsadmin
```

Measurements

These tables list new, modified, or deleted measurements.

Note See the Using BTS Measurements chapter of the *Cisco BTS 10200 Operations and Maintenance Guide, Release 6.0.3* for a complete list of all traffic measurements.

Call Processing Measurements

Table C-4 lists the new call processing measurements provided to support this feature.

Table C-4 Call Processing Measurements Used by Overload Control

Measurement	Description
CALLP_OLM_OFFERED	The total number of calls offered to OLM
CALLP_OLM_ACCEPT	The total number of calls accepted by OLM
CALLP_OLM_REJECT	The total number of calls rejected by OLM
CALLP_OLM_ACCEPT_MCL0	Calls accepted by OLM at MCL0
CALLP_OLM_ACCEPT_MCL1	Calls accepted by OLM at MCL1
CALLP_OLM_ACCEPT_MCL2	Calls accepted by OLM at MCL2
CALLP_OLM_ACCEPT_MCL3	Calls accepted by OLM at MCL3
CALLP_OLM_REJECT_MCL1	Calls rejected by OLM at MCL1
CALLP_OLM_REJECT_MCL2	Calls rejected by OLM at MCL2
CALLP_OLM_REJECT_MCL3	Calls rejected by OLM at MCL3
CALLP_OLM_REJECT_MCL4	Calls rejected by OLM at MCL4
CALLP_OLM_REJECT_EMERGENCY	Emergency calls rejected at MCL4
CALLP_OLM_MCL1_COUNT	Total number of MCL1 occurrences
CALLP_OLM_MCL2_COUNT	Total number of MCL2 occurrences
CALLP_OLM_MCL3_COUNT	Total number of MCL3 occurrences
CALLP_OLM_MCL4_COUNT	Total number of MCL4 occurrences
CALLP_OLM_ISUP_MSG_DUMPED	Number of ISUP messages dumped at MCL4 by layer 3/4 interface (MIM) due to system overload.

Service Interaction Manager Measurements

Table C-5 lists the new Service Interaction Manager measurements provided to support this feature.

Table C-5 Service Interaction Manager Measurements Used by Overload Control

Measurement	Description
SIM_OC_TRIG_FILTERED	The number of triggers dropped when the FS is overloaded (a single counter is used by SIM, which tracks the trigger filtering for all the FS). SIM updates this counter every time it filters a trigger due to congestion on a FS.
SIM_OC_EMG_TRIG_FORCED	The number of emergency triggers (that is, TRIGGER_911) forced when the FS is overloaded. A single counter is used by SIM which tracks number of emergency triggers forced for all the FS. SIM updates this counter every time it forces an emergency trigger (TRIGGER_911) to FS.
SIM_OC_TRIG_FORCED	The number of triggers forced when the FS is overloaded. A single counter is used by SIM which tracks the number of forced triggers for all the FSs. SIM updates this counter every time it forces a trigger.

Traffic Measurements Monitor Counters

Table C-6 lists the new Traffic Measurements Monitor (TMM) measurements provided to support this feature.

Table C-6 TMM Timers Used by Overload Control

Measurement	Description
SIA_OC_RX_INVITE_REJECT	The total number of incoming invite messages rejected by SIA due to overload.
SIA_OC_RX_REGISTER_REJECT	The total number of incoming register messages rejected by SIA due to overload
SIA_OC_RX_REFER_REJECT	The total number incoming refer messages rejected by SIP due to overload.
SIA_OC_RX_SUBSCRIBE_REJECT	The total number of incoming subscribe messages rejected.
SIA_OC_RX_UNSOL_NOTIFY_SUPP	The total number of unsolicited notification requests suppressed without being sent to the endpoints.
SIA_OC_RX_OPTIONS_REJECT	The total number of incoming options messages rejected by SIA due to overload.

Miscellaneous Measurements

Table C-7 lists additional measurements added to support Overload Control.

Table C-7 Miscellaneous Measurements Used by Overload Control

Timer	Description
ISUP_CONG_CALL_REJECTED	The congestion-rejected calls on a per trunk group basis. This is implemented for SGA.
POTS_OC_DP_RECEIVED	The number of Detection Points (DPs) reported during periods of congestion. This is being pegged by the FS.
H323_OC_SETUP_REJECTED	The total number of incoming H.225 Setup messages rejected by the Cisco BTS 10200 due to overload.
MEAS_ISA_OC_SETUP_REJECTED	The number of ISDN calls rejected due to system overload.
MEAS_MGA_OC_CALL_REJECTED	The number of MGCP calls rejected due to system overload.

Troubleshooting

This section lists the Events and Alarms added to support this feature.

Events and Alarms

The FS sends an alarm when:

- MCL changes.
- An individual critical factor reaches its threshold.

The CA sends an Informational alarm when:

- It receives a congested notification.
- It receives an abatement notification from an FS.

Informational alarms are sent at fixed 25 percent increments. A configurable parameter, info_alarm_step_size, is added to each factor defined in olm.cfg. Ensure that the value allows sufficient warning. The default for info_alarm_step_size is 5, giving factor informational alarms at 5, 10, and 15 percent, and so on.

Congestion Status—Maintenance (112)

The Congestion Status alarm (major) indicates that MCL changes have occurred, "System MCL Level." The System MCL Level is the effective MCL or the greater of either the computed MCL or the administrative MCL.

When a new Maintenance (112) alarm appears, the old Maintenance (112) alarm is cleared. When the system MCL falls to 0, the alarm is cleared.

The alarm is dampened using the alarm_damping_time setting in olm.cfg. The value of alarm_damping_time is the minimum amount of time that passes before the alarm is issued after a change has occurred.

For additional information, refer to the "Maintenance (112)" section on page 7-61.

CPU Load of Critical Processes—Maintenance (113)

The CPU Load of Critical Processes alarm (info) indicates that the MCL from the CPU utilization factor crossed a multiple of the info_alarm_step_size. This alarm appears for every crossing of the info_alarm_step_size, but it must pass the next higher or lower level before it is issued again.

For additional information, refer to the "Maintenance (113)" section on page 7-62.

Queue Length of Critical Processes—Maintenance (114)

The Queue Length of Critical Processes alarm (info) indicates that the MCL for defined critical process queue length factors crossed a multiple of the info_alarm_step_size. This alarm is issued for every crossing of the info_alarm_step_size, but it must pass the next higher or lower level before it is issued again.

For additional information, refer to the "Maintenance (114)" section on page 7-62.

IPC Buffer Usage Level—Maintenance (115)

The IPC Buffer Usage Level alarm (info) indicates that the MCL for IPC buffer usage factor crossed a multiple of the info_alarm_step_size. This alarm appears for every crossing of the info_alarm_step_size, but it must pass the next higher or lower level before it is issued again.

For additional information, refer to the "Maintenance (115)" section on page 7-63.

CA Reports the Congestion Level of FS—Maintenance (116)

CA Reports the Congestion Level of FS alarm (info) shows CA received a congestion or abatement notification from an FS.

For additional information, refer to the "Maintenance (116)" section on page 7-63.

Logs

Use the INFO logs to get differing levels of information about the alarms:

- INFO1—Are included with each alarm
- INFO3—Print factor feature controlled by olm.cfg which shows system overview
- INFO4—Have extra detail
- INFO5—Shows exact details of the factor MCL computations

GLOSSARY

Revised: August 10, 2011, OL-25016-01

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

BHCA Busy Hour Call Attempts

BLG billing

BLO blocking

BTS Broadband Telephony Softswitch

BW bandwidth

C

CA Call Agent

CA California

CALLP call processing

CAROT Centralized Automatic Reporting on Trunks

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 memory

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

DPC destination point code

DSCP differentiated service code point

DUPU destination user part unavailable

E

EA equal access

EGA event generator

EM Element Manager

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

FCAPS Fault, Configuration, Accounting, Performance, and Security

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 title translation

GUI Graphical User Interface

GW gateway

H

H323 H.323 Protocol

H323GW H323 gateway

H3A H.323 signaling adapter

HB heartbeat

HSS Home Subscriber Server

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

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

ITL	Incoming Test Line (same as TTL)
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 not facility associated signaling

NFS network file server

NGN Next Generation Networks

NIIF Network Interconnection Interoperability Forum

NML Network Management Layer

NMS network management system

NNN numeric number nomenclature

NOA nature of address

NPA Numbering Plan Area

NPAC Number Portability Administration Center

NR nonrecoverable

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

OTL Originating Test Line

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

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

ROTL Remote Office Test Line

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 retransact

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

SCCS Switched Control Center System

SCP service control point, signal control point

SCTP Stream Control Transmission Protocol

SDH Synchronous Digital Hierarchy

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

SONET Synchronous Optical Network

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
TERMID	Termination Identification
TFC	transfer controlled
TG	trunk group, trunking gateway
TGID or TGN-ID	trunk group ID
TIA	Telecommunications Industry Association
TMM	Traffic and Measurements module
TMN	Telecommunications Management Network (ITU-T)
TOS	type of service
TPM	terminating point master
TRNS	transient
TSA	TCAP signaling adapter
TSAP	transport service access point
TT	translation type
TTL	Terminating Test Line
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

VOA Voice Over ATM

VOIP voice over IP

VOP Voice Over Packet

VTOC volume table of contents

W

X

XUA extended unit association

XUDTS extended unit data service

Y

Z