



CHAPTER 1

Troubleshooting Overview

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

Introduction

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

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

Interoperability

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



Caution

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

Symptoms, Problems, and Solutions

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

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

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

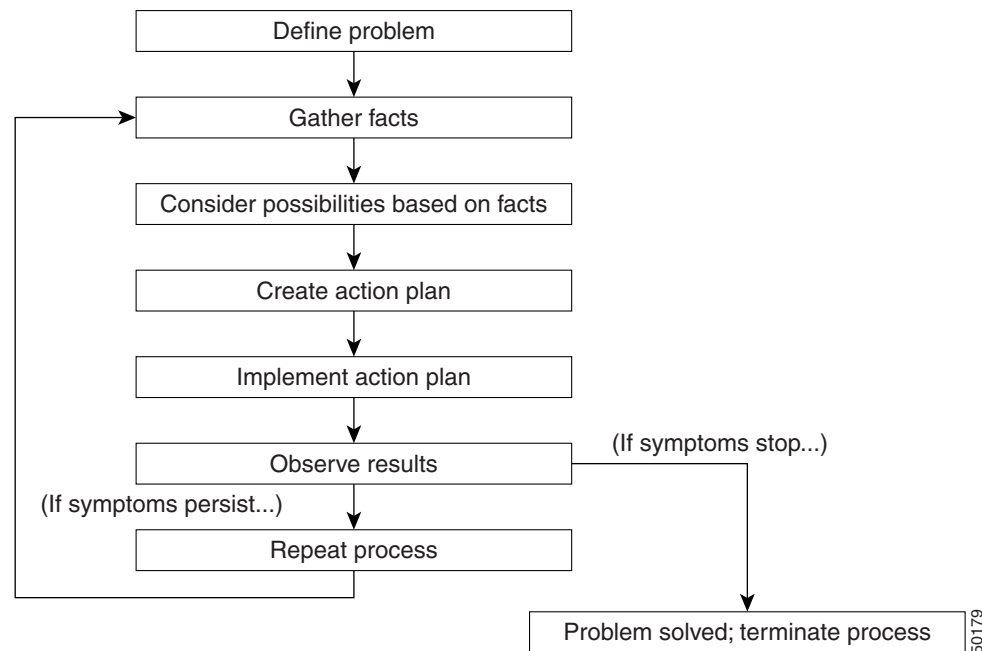
General Problem-Solving Model

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

A systematic approach employs the following steps:

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

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

Figure 1-1 General Problem-Solving Model

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

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

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

**Note**

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

Resolving Network Problems

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

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

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

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

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

Resolving System Problems

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

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

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

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



Caution

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



Caution

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



Caution

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

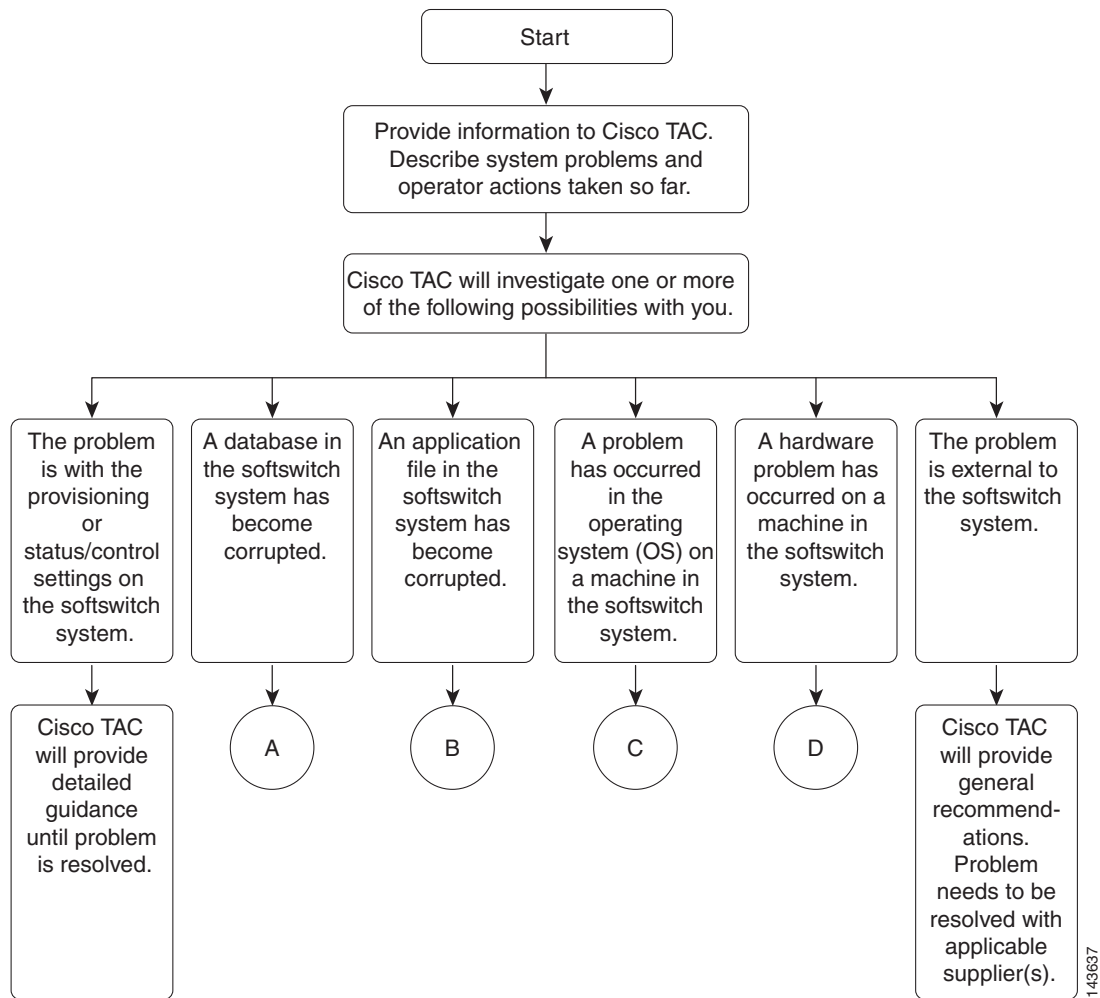
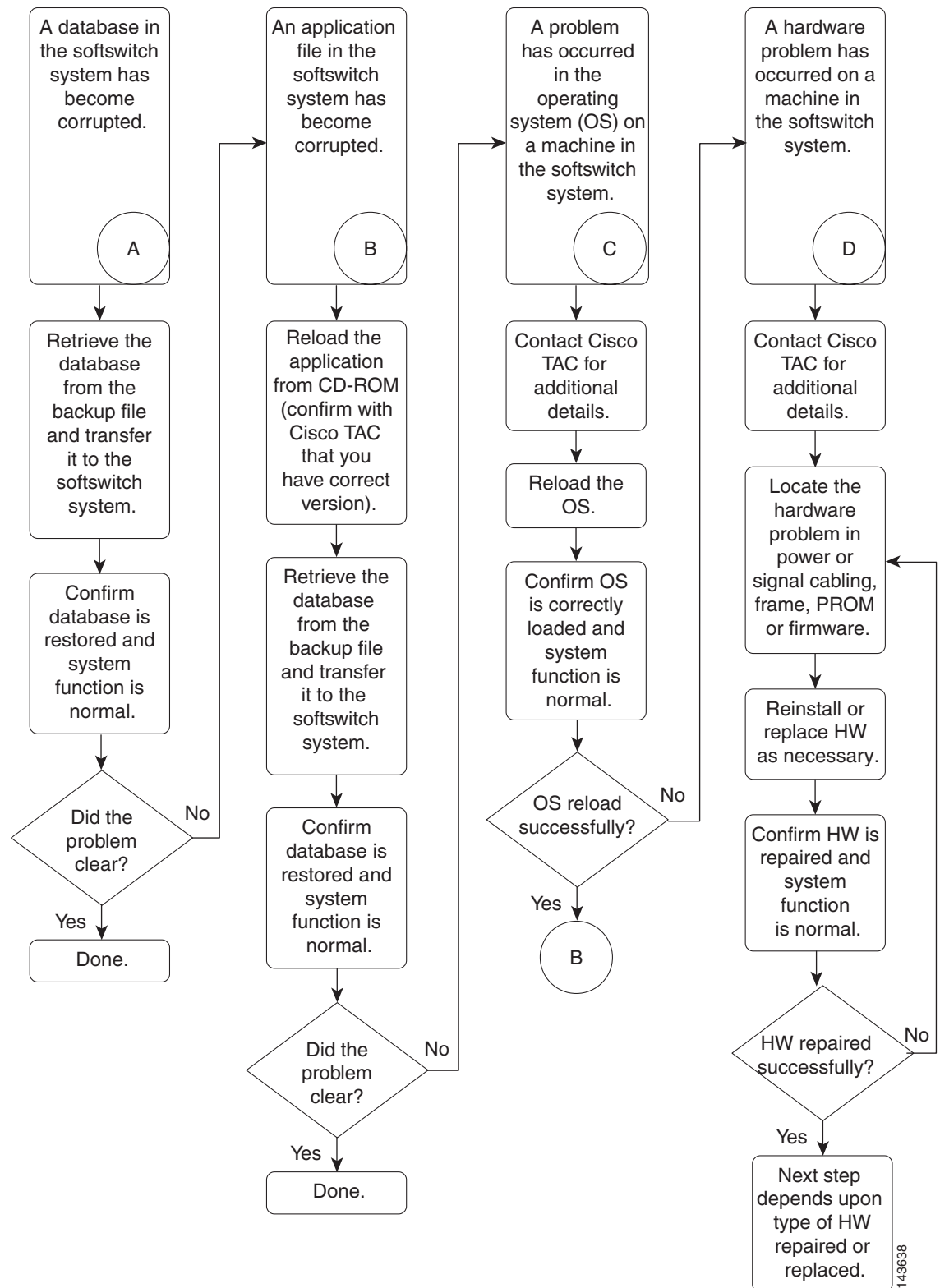
Figure 1-2 Problem Identification

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

143638

Managing Events and Alarms

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

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

Alarms and informational events produce different system responses.

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

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

This section contains the following:

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

**Note**

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

Managing Event and Alarm Reports

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

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

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



Note

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

Show Alarm Command

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

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



Note

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

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

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

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

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

Report Alarm Command

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

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



Note

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

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

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

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

Ack Alarm Command

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

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

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



Note

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

Clear Alarm Command

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

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

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

To clear all alarms, use the following command.

```
clear alarm forced=Y
```



Note

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

Format of Alarm Reports

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

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

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

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

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

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

Events and Alarm Logs

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

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

Viewing Event or Alarm Logs

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

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



Note

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

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

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



Note

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

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

- **id**—The unique serial number of the event or alarm assigned by the system.

- **type**—The type of event or alarm to show, which can be any one of the following:
 - audit
 - billing
 - callp
 - config
 - database
 - maintenance
 - oss
 - security
 - signaling
 - statistics
 - system
- **number**—The numerical identifier of the event or alarm of the specified type (1 to 500).
- **severity**—The severity level of the event or alarm, which can be any one of the following:
 - critical
 - major
 - minor
 - warning (events only)
 - info (events only)
- **origin**—The internal designation of the process generating the event or alarm (1 to 64 ASCII characters).
- **component-id**—The ID of the component reporting the event or alarm (1 to 32 ASCII characters).

Specifying the component-ID, setting type to a value, and specifying a number displays only alarms of that type and number from the designated component.
- **start-time** or **end-time**—The timestamp indicating the time interval for reporting events or alarms in the format <yyyy-mm-dd hh:mm:ss> where:
 - yyyy—year (4-digit number)
 - mm—month (01 to 12)
 - dd—day (01 to 31)
 - hh—hour (00 to 23)
 - mm—minute (00 to 59)
 - ss—second (00 to 59)

Show, Add, and Delete Event Queue Commands

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

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

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

Saving Events to Log Files

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

Show Report-Properties Command

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

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

TYPE=EVENT_LOGSIZE
VALUE=30000

TYPE=ALARM_LOGSIZE
VALUE=30000

TYPE=EVENT_LEVEL
VALUE=INFO
```

**Note**

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

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

Changing Report Properties

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

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

or

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

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

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

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

For example:

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



Tip

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

Changing Threshold and Throttle Values

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

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

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

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

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

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

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

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


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

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

Managing and Responding to Events and Alarms

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

-
- Step 1** Set the **event-logsize** and **event-level** parameters as desired using the **report-properties** command (see the [“Changing Report Properties”](#) section on page 1-15).
- Step 2** Subscribe to events and request event summary reports as needed using the **subscribe** command (see the [“Managing Event and Alarm Reports”](#) section on page 1-9).
- Step 3** Set the **alarm-logsize** and **event-level** parameters as desired using the **report-properties** command (see the [“Changing Report Properties”](#) section on page 1-15).
- Step 4** Subscribe to alarms and request alarm summary reports as needed using the **subscribe** command (see the [“Managing Event and Alarm Reports”](#) section on page 1-9).
- Step 5** Set the **threshold** and **throttle** parameters as desired using the **change event-prov** command (see the [“Changing Threshold and Throttle Values”](#) section on page 1-16).
- Step 6** View event and alarm reports and investigate potential problems.
- Examples of problems to look for include: congestion warnings, routing errors, termination failures, billing errors, diagnostic failures, security warnings, and process failovers.
- Step 7** Refer to the “Probable Cause” and “Corrective Action” instructions for events and alarms in the [“Events and Alarms Descriptions and Corrective Actions”](#) section on page 1-17.
- Step 8** Take the necessary corrective action; escalate the problem if necessary.
- The situation that caused an event or alarm must be resolved before the event or alarm can be cleared.
- Step 9** After the problem is fixed, enter the following command to clear a specific alarm:

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

Where:

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



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

Events and Alarms Descriptions and Corrective Actions

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

Format of Events and Alarms

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

SIGNALING (20) Example

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

Message Type and Number

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

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

- **AUDIT**—Events or alarms generated by the audit subsystem. Refer to [Chapter 2, “Audit Troubleshooting.”](#)
- **BILLING**—Events or alarms generated by the billing subsystem. Refer to [Chapter 3, “Billing Troubleshooting.”](#)
- **CALLP**—Events or alarms generated by call processing. Refer to [Chapter 4, “Call Processing Troubleshooting.”](#)
- **CONFIG**—Events or alarms generated that provide information about system configuration. Refer to [Chapter 5, “Configuration Troubleshooting.”](#)
- **DATABASE**—Events or alarms generated by the database. Refer to [Chapter 6, “Database Troubleshooting.”](#)
- **MAINTENANCE**—Events or alarms that provide information about maintenance. Refer to [Chapter 7, “Maintenance Troubleshooting.”](#)

- **OSS**—Events or alarms generated by the OSS. Refer to [Chapter 8, “Operations Support System Troubleshooting.”](#)
- **SECURITY**—Events or alarms generated by the billing subsystem. Refer to [Chapter 9, “Security Troubleshooting.”](#)
- **SIGNALING**—Events or alarms generated by signaling protocols or interfaces. Refer to [Chapter 10, “Signaling Troubleshooting.”](#)
- **STATISTICS**—Events or alarms that provide information about system statistics. Refer to [Chapter 11, “Statistics Troubleshooting.”](#)
- **SYSTEM**—Events or alarms that convey information about system status or trouble. Refer to [Chapter 12, “System Troubleshooting.”](#)

Event Level

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

- **CRITICAL**—Service can be severely affected and an alarm is raised. A critical alarm indicates a critical situation exists somewhere in the system. Critical alarms can cause failovers (active server switches processing to standby server). Critical alarms must be investigated and cleared immediately.
- **MAJOR**—Service can be degraded and an alarm is raised. A major alarm indicates that a serious situation exists that can disrupt service. Major alarms differ from critical alarms in that they usually do not cause failovers. Major alarms should also be investigated and cleared immediately.
- **MINOR**—Service (call processing) is not affected; however, an alarm is raised. Minor alarms should be noted and cleared as soon as possible.
- **WARNING**—Warning messages provide cautionary advice about a potential service impact. They indicate conditions that should be investigated immediately to ensure that the situation does not progress into an alarmed state.
- **INFO**—Informational events indicate various stages of system operation as well as atypical network conditions, such as timer expirations, values that have exceeded preset thresholds, or unexpected responses from endpoints to signaling messages sent by the Cisco BTS 10200 Softswitch.

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

Threshold/Throttle

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

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

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

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

Data Reported

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

Probable Cause

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

Corrective Action

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