CHAPTER 2

Alarms and Events

Revised: July 24, 2009, OL-3743-42

This chapter describes Cisco BTS 10200 Softswitch alarms and events. This chapter is divided into three parts:

- Alarm or Event Log Command—The Log command is valid for both alarms and events.
- Alarms—Valid alarm commands.
- Events—Valid event commands.

Note In this chapter, an asterisk preceding a token name means the token is mandatory. A token without an asterisk is optional.

Alarm or Event Log Command

This command is valid for both alarms and events. The Alarm Log command requests a summary report of alarms by severity, type, and start/stop times from the Alarm Log (alarm-log) table. Alarms are events with severities of minor, major, or critical. Substituting Event for Alarm returns a summary report of events by severity, type, and start/stop times from the Event Log (event-log) table.

Table Name: ALARM-LOG or EVENT-LOG

Table Containment Area: OAMP

Command Types Show

Examples

```
show alarm-log
show event-log
```

Usage Guidelines Primary Key Token(s): id

Change Rules: None.

Syntax Description

ID (System generated)	Primary key. A unique integer value that identifies the specific event or alarm in the log. INTEGER: 12-digit number.
TYPE	Type of event to show in the alarm summary. Only one type is selectable at a time. VARCHAR(12): 1–12 ASCII characters. Permitted values are: AUDIT (Audit events)—Events dealing with audit. This includes the starting and stopping of an audit, depending on how the audit was defined. BILLING (Billing data alarms)—This includes the generation, collection, and retrieval of billing call events. CALLP (Call processing alarms)—Alarm types dealing with the processing of actual call data. CONFIG (Configuration alarms)—Alarm types dealing with the provisioning aspects of the system. Includes all activity such as system devices and facility management. DATABASE (Database alarms)—Alarm types dealing with database activity. Includes table download, reading, and writing. MAINTENANCE (Maintenance alarms)—Alarm types dealing with fault handling and diagnostic areas. Includes test facilities and the health of hardware and software components. OSS (Operating system services)—Alarm types dealing with the Cisco BTS 10200 Softswitch external interfaces that are on the northbound side of the system. This does not include southbound components in the system. SECURITY (Security alarms)—Alarm types dealing with access to the system through both human interfaces and machine interfaces. SIGNALING (Signaling alarms)—Alarm types dealing with protocol stacks such as MGCP and TDM interfaces like SS7. STATISTICS (Statistical alarms)—Alarm types dealing with the accumulation, collection, and reporting of measurements in the system. This includes traffic and performance data. SYSTEM (System events)—Events dealing with the system. This includes events dealing with low-level process activities, such as the IDX table reads and IPC messaging.
ALARM-STATUS	Status of an alarm. VARCHAR(12): 1–12 ASCII characters. Permitted values are: ON OFF ACKNOWLEDGED IGNORED

AUTO-REFRESH	Specifies whether to display cached data on the screen. Valid only for the show command. CHAR(1): Y/N (Default = Y). Y—Queries the database for the most current data. N—Queries the database for the most current data only if the cached data is unavailable.
DISPLAY	Specifies what token information to display on the screen. Valid only for the show command. VARCHAR(51200): 1–51200 (Default = all tokens are displayed). Permitted values are any valid token that can be shown for this command. Multiple tokens can be entered by separating with a comma.
END-TIME	Ending time for alarm summary. Enter all 19 ASCII characters as shown. DATE: YYYY-MM-DD HH:MM:SS.
LIMIT	Specifies the number of rows to display on the screen. Valid only for the show command. INTEGER: 1–100000000 (Default = 100000000). **Note** The actual maximum number of rows displayed is currently lower than 100000000 due to software limitations.
NUMBER	Numerical identifier of the event to clear or query. NUMERIC: 1–150. NUMERIC: 1–500 (Release 4.5).
ORDER	Specifies whether to display data on the screen in a sorted order. Valid only for the show command. VARCHAR(51200): 1–51200 (Default = all rows are displayed). Permitted values are any valid token that can be shown for this command. Multiple tokens can be entered by separating with a comma.
ORIGIN	Process that originated the alarm, for example: pmg, mga, and so forth. VARCHAR(12): 1–12 ASCII characters.

SEVERITY	Level of alarm or event to show in the summary. VARCHAR(8): 1–8 ASCII characters. Permitted values are: INFO (Information level)—Provides only added data to the general processing of an event report. Selecting Info turns on Info and all the levels above it (Warn, Minor, Major, and Critical). WARNING (Warning level)—Indicates that some potential service degradation is occurring as a result of internal or external processing. At this level, processing is able to continue. Turns on Warn and all the levels above it (Minor, Major, and Critical). MINOR (Minor level)—Indicates that some loss of capacity or availability has occurred. An example is the loss of an Ethernet link or a software outage. Selecting Minor turns on Minor and all the levels above it (Minor, Major, and Critical). MAJOR (Major level)—Indicates a loss of capacity or availability. It refers to a larger loss than Minor or an escalation of some earlier alarm. Selecting Major turns on Major and Critical. CRITICAL (Critical level)—Indicates a catastrophic condition in the system that requires operator attention and potential supervision over the situation. This can be an outage or complete loss of service somewhere in the system. Selecting Critical turns on Critical only.
START-ROW	Specifies to begin displaying data on the screen at a specific row. Valid only for the show command. INTEGER: 1–100000000 (Default = 1).
START-TIME	Starting time for alarm summary. Enter all 19 ASCII characters as shown. Start-time must occur before end-time. Alarm events are available for the current and previous calendar days only. Level indicates the minimum level to show in the report summary. DATE: YYYY-MM-DD HH:MM:SS.

Alarm or Event Report Properties

The Report Properties (report-properties) command (formerly Alarm-logsize or Event-logsize) specifies the maximum number of alarm or event entries permitted (up to 30,000) in the Report Properties (report-properties) table. It also specifies the minimum event severity level to be stored in the Event Log.

Table Name: REPORT-PROPERTIES

Table Containment Area: OAMP

Command Types Show and change

Examples

```
show report-properties;
```

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

```
change report-properties type=alarm-logsize; value=1234
change report-properties type=event-logsize; value=5000
```

Usage Guidelines

Primary Key Token(s): None.

Change Rules: None.

Syntax Description

TYPE	Optional for show; mandatory for change. Primary key. Type of alarm or event. VARCHAR(12): 1–12 ASCII characters. Permitted values are: ALARM-LOGSIZE EVENT-LOGSIZE EVENT-LEVEL
VALUE	Optional for show; mandatory for change. Property value. Do not enter commas. VARCHAR(12): 1–12 ASCII characters. For type=alarm-logsize or event-logsize, valid values are 1–30000. For type=event-level, valid values are INFO, WARNING, MINOR, MAJOR, CRITICAL (or the minimum level of events stored in the log).
AUTO-REFRESH	Specifies whether to display cached data on the screen. Valid only for the show command. CHAR(1): Y/N (Default = Y). Y—Queries the database for the most current data. N—Queries the database for the most current data only if the cached data is unavailable.
DISPLAY	Specifies what token information to display on the screen. Valid only for the show command. VARCHAR(51200): 1–51200 (Default = all tokens are displayed). Permitted values are any valid token that can be shown for this command. Multiple tokens can be entered by separating with a comma.
LIMIT	Specifies the number of rows to display on the screen. Valid only for the show command. INTEGER: 1–100000000 (Default = 100000000). **Note** The actual maximum number of rows displayed is currently lower than 100000000 due to software limitations.
ORDER	Specifies whether to display data on the screen in a sorted order. Valid only for the show command. VARCHAR(51200): 1–51200 (Default = all rows are displayed). Permitted values are any valid token that can be shown for this command. Multiple tokens can be entered by separating with a comma.
START-ROW	Specifies to begin displaying data on the screen at a specific row. Valid only for the show command. INTEGER: 1–100000000 (Default = 1).

Alarms

Alarms are a subset of events and indicate a problem with the system.

Alarm

The Alarm (alarm) command shows, clears, and acknowledges specific alarms on specific nodes.

Table Name: ALARM

Table Containment Area: OAMP

Command Types

Show, ack, and clear

Examples

```
show alarm;
clear alarm id=123;
ack alarm id=123;
```

Usage Guidelines

Primary Key Token(s): id

Change Rules: None.

Syntax Description

ID (System generated)	Primary key. A unique integer value that identifies the specific alarm in the log. INTEGER: 12-digit number.
AUTO-REFRESH	Specifies whether to display cached data on the screen. Valid only for the show command. CHAR(1): Y/N (Default = Y). Y—Queries the database for the most current data. N—Queries the database for the most current data only if the cached data is unavailable.
DISPLAY	Specifies what token information to display on the screen. Valid only for the show command. VARCHAR(51200): 1–51200 (Default = all tokens are displayed). Permitted values are any valid token that can be shown for this command. Multiple tokens can be entered by separating with a comma.
END-TIME	Ending time for alarm summary. Enter all 19 ASCII characters as shown. DATE: YYYY-MM-DD HH:MM:SS.
LIMIT	Specifies the number of rows to display on the screen. Valid only for the show command. INTEGER: 1–100000000 (Default = 100000000). **Note** The actual maximum number of rows displayed is currently lower than 100000000 due to software limitations.

NUMBER	Numerical identifier of the alarm to clear or query. INTEGER: 1–200.
ORDER	Specifies whether to display data on the screen in a sorted order. Valid only for the show command. VARCHAR(51200): 1–51200 (Default = all rows are displayed). Permitted values are any valid token that can be shown for this command. Multiple tokens can be entered by separating with a comma.
START-ROW	Specifies to begin displaying data on the screen at a specific row. Valid only for the show command. INTEGER: 1–100000000 (Default = 1).
START-TIME	Starting time for alarm summary. Enter all 19 ASCII characters as shown. Start-time must occur before end-time. Alarm events are available for the current and previous calendar days only. Level indicates the minimum level to show in the report summary. DATE: YYYY-MM-DD HH:MM:SS.

Alarm Report

The Alarm Report (alarm-report) command provides the ability to subscribe or unsubscribe to each level and type of alarm report.

Table Containment Area: OAMP

Command Types

Subscribe and unsubscribe

Note When you subscribe to alarms or events, they take over the screen as they happen, which can interrupt other commands.

Examples

```
subscribe alarm-report severity=major; type=callp,config;
unsubscribe alarm-report severity=major,critical; type=all;
```

Usage Guidelines

Primary Key Token(s): None.

Syntax Description

SEVERITY	Specifies the minimum severity of an alarm report to subscribe to or unsubscribe from. VARCHAR(8): 1–8 ASCII characters. Permitted values are: MINOR (Minor severity)—Indicates that some loss of capacity or availability occurred. An example is the loss of an Ethernet link or a software outage. Selecting Minor turns on Minor and all the levels above it (Minor, Major, and Critical). MAJOR (Major severity)—Indicates a loss of capacity or availability. This is a larger loss than Minor or an escalation of an earlier alarm. Selecting Major turns on Major and Critical. CRITICAL (Critical severity)—Indicates a catastrophic condition in the system that requires operator attention and potential supervision over the situation. This can be an outage or a complete loss of service somewhere in the system. Selecting Critical only turns on Critical. ALL—Turns on all severities.
TYPE	Type of alarm report to subscribe to or unsubscribe from. VARCHAR(12): 1–12 ASCII characters. Permitted values are: AUDIT (Audit events)—Events dealing with audit. This includes the starting and stopping of an audit, depending on how the audit was defined. BILLING (Billing alarms)—Alarms dealing with bill data. This includes the generation, collection, and retrieval of billing call events. CALLP (Call processing alarms)—Alarm types dealing with the processing of actual call data. CONFIG (Configuration alarms)—Alarm types dealing with the provisioning aspects of the system. Includes all activity such as system devices and facility management. DATABASE (Database alarms)—Alarm types dealing with database activity. Includes table download, reading, and writing. MAINTENANCE (Maintenance alarms)—Alarm types dealing with fault handling and diagnostic areas. Includes test facilities and the health of hardware and software components. OSS (Operating System Services)—Alarm types dealing with the Cisco BTS 10200 Softswitch external interfaces that are on the northbound side of the system. This does not include southbound components in the system. SECURITY (Security alarms)—Alarm types dealing with access to the system through both human interfaces and machine interfaces. SIGNALING (Signaling alarms)—Alarm types dealing with protocol stacks such as MGCP and TDM interfaces such as SS7. STATISTICS (Statistical alarms)—Alarm types dealing with the accumulation, collection, and reporting of measurements in the system. This includes traffic and performance data. SYSTEM (System events)—Events dealing with the system. This includes events dealing with low-level process activities, such as the IDX table reads and IPC messaging. ALL—Turns on all of the above.

Events

Cisco BTS 10200 Softswitch events are indications that something has happened with the system.

Event Provisioning

The Event Provisioning (event-prov) command uses the Report Parameters (reportparameters) table to provision threshold and throttling values for any event that can be issued by the system.

Table Name: REPORTPARAMETERS

Table Containment Area: OAMP

Command Types

Show and change

Examples

```
show event-prov type=callp; number=20;
```

Note The show command also displays the descriptive string and the data labels for the specified data words.

```
change event-prov type=callp; number=20; threshold=95; throttle=1;
```

Usage Guidelines

Primary Key Token(s): type, number

Change Rules: None.

Other Rules: Type and number are the only valid tokens for this command. The limit, start-row, display, order, threshold and throttle tokens cannot be used with the show event-prov command—returns the error message “invalid key(s) found.”

Syntax Description

NUMBER	Primary key. Unique instance within the event category. NUMERIC: 1–200.
TYPE	Primary key. Event category. VARCHAR(12): 1–12 ASCII characters. Permitted values are: CALLP (Call processing events)—Events dealing with the processing of actual call data. CONFIG (Configuration events)—Events dealing with the provisioning aspects of the system. Includes all activity such as system devices and facility management. DATABASE (Database events)—Events dealing with database activity. Includes table download, reading, and writing. MAINTENANCE (Maintenance events)—Events dealing with fault handling and diagnostic areas. Includes test facilities and the health of hardware and software components. OSS (Operating System Services events)—Events dealing with the Cisco BTS 10200 Softswitch external interfaces that are on the northbound side of the system. This does not include southbound components in the system. SECURITY (Security events)—Events dealing with access to the system through both human interfaces and machine interfaces. SIGNALING (Signaling events)—Events dealing with protocol stacks such as MGCP and TDM interfaces like SS7. STATISTICS (Statistical events)—Events dealing with the accumulation, collection, and reporting of measurements in the system. This includes traffic and performance data. BILLING (Billing events)—Events dealing with billing data. This includes the generation, collection, and retrieval of billing call events. AUDIT (Audit events)—Events dealing with audit. This includes the starting and stopping of an audit, depending on how the audit was defined. SYSTEM (System events)—Events dealing with the system. This includes events dealing with low-level process activities, such as the IDX table reads and IPC messaging.
AUTO-REFRESH	Specifies whether to display cached data on the screen. Valid only for the show command. CHAR(1): Y/N (Default = Y). Y—Queries the database for the most current data. N—Queries the database for the most current data only if the cached data is unavailable.
DISPLAY	Specifies what token information to display on the screen. Valid only for the show command. VARCHAR(51200): 1–51200 (Default = all tokens are displayed). Permitted values are any valid token that can be shown for this command. Multiple tokens can be entered by separating with a comma.

LIMIT	Specifies the number of rows to display on the screen. Valid only for the show command. INTEGER: 1–100000000 (Default = 100000000). **Note** The actual maximum number of rows displayed is currently lower than 100000000 due to software limitations.
ORDER	Specifies whether to display data on the screen in a sorted order. Valid only for the show command. VARCHAR(51200): 1–51200 (Default = all rows are displayed). Permitted values are any valid token that can be shown for this command. Multiple tokens can be entered by separating with a comma.
START-ROW	Specifies to begin displaying data on the screen at a specific row. Valid only for the show command. INTEGER: 1–100000000 (Default = 1).
THRESHOLD	Mandatory for change. Specifies the maximum number of events, (as identified by its type and number) to be reported for a 30-minute interval. Specifying the value zero establishes no threshold; therefore, every event of the specified type and number would be reported during the 30-minute interval. Specifying the default value of 100 would enable the Cisco BTS 10200 Softswitch to report the first 100 events of the specified type and number during the 30-minute interval but no more until the beginning of the next interval. If both the threshold and throttle parameters are specified, the throttle parameter is applied before the threshold parameter is considered. NUMERIC: 0–100 (Default = 100).
THROTTLE	Mandatory for change. Reporting reduction factor. For any throttle value, *n*, the system issues only one report for every *n* event for the specified event. When setting both throttle and threshold, the throttle value is applied before the threshold values. NUMERIC: 0–100 (Default = 0). A throttle set to zero means no throttling.

Event Report

The Event Report (event-report) command provides the ability to view events in a near real-time format by subscribing or unsubscribing to each level and type of event report.

Table Containment Area: OAMP

Command Types

Subscribe and unsubscribe

Examples

```
subscribe event-report severity=info; type=callp;
```

Note When you subscribe to alarms or events, they take over the screen as they happen, which can interrupt other commands.

```
unsubscribe event-report severity=info, warn; type=callp;
```

Usage Guidelines Primary Key Token(s): None.

Syntax Description

SEVERITY	Specifies the minimum severity of event report to be subscribed to or unsubscribed from. VARCHAR(8): 1–8 ASCII characters. Permitted values are: INFO (Information severity)—Provides only added data to the general processing of an event report. Selecting Info turns on Info and all the levels above it (Warn, Minor, Major, and Critical). WARNING (Warning severity)—Indicates that some potential service degradation is occurring as a result of internal or external processing. At this level, processing is able to continue. Turns on Warn and all the levels above it (Minor, Major, and Critical). MINOR (Minor severity)—Indicates some loss of capacity or availability has occurred. An example is the loss of an Ethernet link or a software outage. Selecting Minor turns on Minor and all the levels above it (Major and Critical). MAJOR (Major severity)—Indicates a loss of capacity or availability. It refers to a larger loss than Minor or an escalation of some earlier alarm. Selecting Major turns on Major and Critical. CRITICAL (Critical severity)—A catastrophic condition in the system that requires operator attention and potential supervision over the situation. This can be an outage or complete loss of service somewhere in the system. Selecting Critical turns on Critical only. ALL—Turns on all severities.

TYPE	Type of event report to be subscribed to or unsubscribed from. VARCHAR(12): 1–12 ASCII characters. Permitted values are: CALLP (Call processing events)—Events dealing with the processing of actual call data. CONFIG (Configuration events)—Events dealing with the provisioning aspects of the system. Includes all activity such as system devices and facility management. DATABASE (Database events)—Events dealing with database activity. Includes table download, reading, and writing. MAINTENANCE (Maintenance events)—Events dealing with fault handling and diagnostic areas. Includes test facilities and the health of hardware and software components. OSS (Operating System Services events)—Events dealing with the Cisco BTS 10200 Softswitch external interfaces that are on the northbound side of the system. This does not include southbound components in the system. SECURITY (Security events)—Events dealing with access to the system through both human interfaces and machine interfaces. SIGNALING (Signaling events)—Events dealing with protocols stacks such as MGCP and TDM interfaces like SS7. STATISTICS (Statistical events)—Events dealing with the accumulation, collection, and reporting of measurements in the system. This includes traffic and performance data. BILLING (Billing data events)—This includes the generation, collection and retrieval of billing call events. AUDIT (Audit events)—Events dealing with audit. This includes the starting and stopping of an audit, depending on how the audit was defined. SYSTEM (System events)—Events dealing with the system. This includes events dealing with low-level process activities, such as the IDX table reads and IPC messaging. ALL—Report all events.