



**NORTEL**

Nortel Business Communications Manager 450 1.0

# Fault and Performance Management

Release 1.0

Document Revision 01.01

---

NN40160-701

Document status: Standard  
Document issue: 01.01  
Document date: August 2008  
Product release: BCM450 1.0  
Job function: Fault and Performance  
Type: Technical Publication  
Language type: EN

Copyright © 2008 Nortel Networks.  
All Rights Reserved.

NORTEL, the globemark design, and the NORTEL corporate logo are trademarks of Nortel Networks.

---

# Contents

---

<b>New in this release</b>	<b>7</b>
Features	7
Fault management	7
System metrics	7
Telephony metrics	7
LED status	7
Alarms	7
<b>Introduction</b>	<b>9</b>
<b>Fault and performance management fundamentals</b>	<b>11</b>
BCM450 fault management scope	11
BCM450 alarms	12
Alarms and log files	12
Alarm severities	12
Alarm administration	12
Alarms & the Alarms Panel	13
Alarm banner	13
Alarm set	14
Alarms and LEDs	15
SNMP traps manager for remote monitoring	16
Alarm configuration scope	17
<b>Using the BCM450 fault management system</b>	<b>19</b>
Administering alarms	19
Monitoring an alarm condition	19
Acknowledging an alarm	20
Clearing the alarm log	21
Using the alarm banner	21
Including or omitting acknowledged alarms in the Alarm Banner	21
Using the alarm set	22
Configuring the alarm set	22
Clearing an alarm from the alarm set	22
Responding to LED indicators	22
Reset the status LED	22

Configuring alarm behaviour	23
Enabling or disabling SNMP traps for alarms	23
Enabling or disabling monitoring for selected alarms	24
Monitoring settings for the alarm set	24
Testing an alarm	25
<hr/>	
<b>Alarm Severity reference</b>	<b>27</b>
Alarm Severities	27
Default mapping of severity levels	27
Alarm graph colours in Element Manager	28
<hr/>	
<b>System metrics monitoring</b>	<b>29</b>
QoS Monitoring	29
Configuring the QoS monitor	31
Configuring QoS logging attributes	31
Viewing QoS logs	32
UPS metrics	33
Accessing the UPS status	34
NTP metrics	34
Accessing the NTP metrics	35
<hr/>	
<b>Telephony metrics monitoring</b>	<b>37</b>
Proactive Voice Quality Management	37
Setting the PVQM threshold settings	39
Viewing PVQM telephony metrics	43
Activity Reporter Basic	44
Enabling Activity Reporter Basic	44
Disabling Activity Reporter Basic	45
Trunk module metrics	46
Viewing the trunk module status	46
Viewing performance history information	46
Viewing D-channel information	47
Disabling or enabling a B-channel setting	47
Provisioning a PRI B-channel	48
Trunk module CSU statistics	48
BCM450 trunk module CSU statistics navigation	49
Enabling the internal CSU	50
Checking the performance statistics	50
Checking the CSU alarms	51
Checking carrier failure alarms	51
Checking bipolar violations	52
Checking short-term alarms	53
Checking defects	53
Viewing CSU alarm history	54
CbC limit metrics	54

Accessing CbC limit metrics	54
Clearing CbC limit metrics	56
Hunt group metrics	56
Accessing Hunt Group metrics	56
Resetting the Hunt Group metrics	58
PSTN Fallback metrics	58
Accessing PSTN Fallback metrics	58
Resetting PSTN Fallback metrics	59
<hr/>	
<b>System LEDs reference</b>	<b>61</b>
System status monitor LEDs	61
<hr/>	
<b>List of alarms</b>	<b>63</b>



---

# New in this release

---

This is the initial release of the BCM450 platform. This document contains information about the alarms and performance metrics supported in the BCM450 system in Release 1.0.

## Navigation

- [Features \(page 7\)](#)

## Features

This document contains information about the following features in Release 1.0.

### Fault management

You can view and manage alarms and SNMP traps on the system. For more information, see [Using the BCM450 fault management system \(page 19\)](#).

### System metrics

You can view detailed information about the performance of the BCM450 and about the performance of system resources. For more information, see [System metrics monitoring \(page 29\)](#).

### Telephony metrics

You can view detailed information about the performance of telephony services on the BCM450 system. For more information, see [Telephony metrics monitoring \(page 37\)](#).

### LED status

The LEDs on the BCM450 hardware provide information about the status of the system. For more information, see [System LEDs reference \(page 61\)](#).

### Alarms

This document provides a list of alarms supported on the BCM450 system. For detailed information about the alarms, see [List of alarms \(page 63\)](#).





---

# Introduction

---

This document contains information about how to manage alarms generated by the BCM450 system and administer alarm settings.

## Navigation

- [Fault and performance management fundamentals \(page 11\)](#)
- [Using the BCM450 fault management system \(page 19\)](#)
- [Alarm Severity reference \(page 27\)](#)
- [System metrics monitoring \(page 29\)](#)
- [Telephony metrics monitoring \(page 37\)](#)
- [System LEDs reference \(page 61\)](#)
- [List of alarms \(page 63\)](#)



---

# Fault and performance management fundamentals

---

This section provides information contains information about managing alarms generated by the system and administering alarm settings.

## Navigation

- [BCM450 fault management scope \(page 11\)](#)
- [BCM450 alarms \(page 12\)](#)
- [Alarm administration \(page 12\)](#)
- [Alarms and LEDs \(page 15\)](#)
- [SNMP traps manager for remote monitoring \(page 16\)](#)
- [Alarm configuration scope \(page 17\)](#)

## BCM450 fault management scope

You can view and manage real-time alarms generated by the BCM450 system. Alarms arise from components that run on the system; these alarms indicate faults or informational conditions that may require resolution from the system administrator. Examples of alarm conditions include:

- a T1 circuit on the system is down
- an administrator stopped a service that runs on the BCM450

You can receive alarm information through any of the following means:

- the Alarms Panel in the BCM450 Element Manager
- the Alarm Banner in the BCM450 Element Manager
- core telephony alarms on the alarm set
- Simple Network Management Protocol (SNMP) traps for remote management of faults

You can manage alarms and alarm information by:

- configuring alarm settings, for example, filter alarms so that only the desired subset of alarms display in the BCM450 Element Manager Alarms Panel are sent as SNMP traps
- administering alarms, for example, acknowledge selected alarms and clear the alarm log

### BCM450 alarms

Software components that run on the BCM450 system generate alarms related to BCM450 services and applications.

Each component includes a range of alarm IDs, so each BCM450 alarm retains a unique alarm ID.

#### Alarms and log files

The system logs all alarms that appear in the BCM450 Element Manager Alarms Panel in the `alarms.systemlog` file. This file is capped at 1 MB in size; when the file reaches this size, the system creates a new `alarms.systemlog` file. The BCM450 keeps the current file as well as three previous files. A new file starts when the BCM450 system reboots.

You can retrieve the `alarms.systemlog` files (the current file and the three previous files) from the BCM450 system using the Log Management task in the BCM450 Element Manager. You can view the files using the BCM450 Log Browser. For more information, see the *BCM450 Administration and Security Guide* (NN40160-601).

#### Alarm severities

By default, alarms display in the Alarm Banner. The BCM450 sends SNMP traps for alarms with a severity of Major and Critical with the exception of PVQM alarms; for these alarms, the BCM sends SNMP traps for all severity levels.

### Alarm administration

Alarm information can be delivered to you by any of the following means:

- on a table on the alarms panel
- on the alarm banner on the bottom right corner of the Element Manager
- on the alarm set

## Alarms & the Alarms Panel

You can view real-time alarm information using the Alarms Panel in the BCM450 Element Manager. Each alarm has a unique identifier. Alarms are displayed in the Alarms table, sorted by date and time by default, with the newest at the top of the table. The Alarms table displays from 50 to 400 alarms. For information about modifying the maximum number of alarms that are displayed, see [Configuring the alarm set \(page 22\)](#). The Alarms table contains the following elements:

- Time — the date and time of the alarm
- Alarm Acked — indicates whether the BCM Element Manager has acknowledged the alarm.
- Alarm ID — the unique alarm ID associated with the alarm
- Severity — the severity of the alarm (Critical, Major, Minor, Warning, and Information)
- Problem Description — a description of the alarm condition
- Component ID — the process that has generated the alarm, in a 3-part DN format. The component ID always identifies the system as a BCM, includes the name of the system that generated the alarm, and identifies the component that generated the alarm. In this way, remote monitoring stations can easily identify what type of system generated an SNMP trap and which system generated the trap.

When you select an alarm in the table, an Alarm Details pane is displayed for the selected alarm. The Alarm Details pane displays the following information:

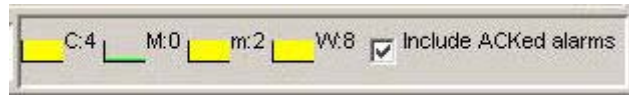
- Time — the date and time of the alarm
- Problem description — a description of the alarm condition
- Problem resolution — the course of action for the alarm

You can acknowledge an alarm to indicate that you have taken care of the alarm. You can specify whether to include acknowledged alarms in the Alarm Banner so that the alarm count remains concise. For more information about the Alarm Banner, see [Alarm banner \(page 13\)](#).

## Alarm banner

You can use the Alarm Banner in the BCM450 Element Manager to view current alarm counts and recent alarm activity on the BCM450 system. The Alarm Banner appears on the bottom-right corner of the BCM450 Element Manager window. The Alarm Banner is visible at all times, so you do not have to navigate to the Alarms Panel to view alarms. If you notice a change in alarm conditions in the Alarm Banner — for example a red spike in the Critical category — you can navigate to the Alarms Panel to view the actual alarm.

### Alarm banner



The Alarm Banner provides counts of Critical, Major, Minor, and Warning alarms; Information alarms are not included. You can specify whether to include acknowledged alarms in the Alarm Banner.

Each alarm severity counter has a graph, which represents a data sample of the last 20 polling intervals. The graph has a color to indicate a data change. The colors are as follows:

**Table 1 Alarm graph colours**

Color	Indicates
Green	There are no alarms of this severity, or there are alarms of this severity but the count has decreased since the last polling interval.
Yellow	There are alarms of this severity, but they are older than at least 1 polling interval.
Red	A new alarm has occurred since the last polling interval.

The system polls for new alarms every 30 seconds by default.

If you clear the alarm log from the BCM450 Element Manager, the alarms displayed on the Alarm Banner are also cleared and reset to 0.

### Alarm set

You can view core telephony alarms on a telephone set on the BCM450 system. This allows a system administrator to monitor alarm activity without having a BCM450 Element Manager and a personal computer.

You can specify the telephone to serve as the alarm set in the BCM450 Element Manager. The telephone set used for alarms must have a 2-line display and three soft keys.

The alarm set displays an alarm as follows:

XXXXX-YYYY

Where XXXXX is the alarm ID and YYYY is additional alarm information.

The following options are available when an alarm is generated to the alarm set:

- Time — indicates the date and time when the alarm occurred
- Clear — use this soft key to remove the alarm from the alarm set.

---

**Attention:** Clearing an alarm from the alarm set does not change the status of alarms on the BCM450 Element Manager or reset the LEDs on the front pane of the unit.

---

---

**Attention:** When an alarm is displayed on the alarm set, it remains visible until you clear the alarm using a softkey on the alarm set. More recent alarms will not be displayed until the current alarm is cleared on the alarm set.

---

The following figure shows an example of an alarm on the alarm set.

**Figure 1 Alarm set alarm**



## Alarms and LEDs

When an alarm condition occurs on the system, the Status LED on the front of the Nortel Business Communications Manager 450 1.0 main unit changes to reflect the alarm condition. In normal operation, both LEDs are green. All alarms with a severity of Major and Critical change the Status LED to solid red on the Nortel Business Communications Manager 450 1.0 front pane, except in the event of a Failed Startup Profile, which is indicated by a flashing red LED.

Using the Nortel Business Communications Manager 450 1.0 Element Manager, you can reset the Status LEDs on the front pane of the Nortel Business Communications Manager 450 1.0 to a normal state.

For information about LEDs and what they indicate, see [System LEDs reference \(page 61\)](#).

---

**Attention:** Once the Status LED has changed to red in response to a Critical or Major alarm condition, it remains in the alarmed state until you reset it using the Nortel Business Communications Manager 450 1.0 Element Manager.

---

### SNMP traps manager for remote monitoring

You can use an SNMP trap manager to remotely monitor BCM450 alarms via SNMP traps. A trap is an indication from the BCM450 system to configured trap managers that an alarm has occurred in the BCM450 system. Any BCM450 alarm can generate an SNMP trap.

If you want the BCM450 to send SNMP traps, you must first configure the SNMP agent using the BCM450 Element Manager. You must enable an SNMP agent and then configure how the system handles SNMP trap notifications. For information about configuring SNMP settings, see [Enabling or disabling SNMP traps for alarms \(page 23\)](#).

The BCM450 system uses the Small Site Events Management Information Base (MIB) for alarms. The trap format is specified in this MIB. You capture and view traps using any standard SNMP fault monitoring framework or trap watcher.

By default, the BCM450 sends SNMP traps for alarms with a severity of Major and Critical. The only exception is PVQM alarms; for these alarms, the BCM send SNMP traps for all severity levels. You can change the default alarms that are set for SNMP to limit the volume and type of SNMP information, and to control essential information that is transferred on the network. For information about how to change the default alarms, see [Configuring the alarm set \(page 22\)](#).



## Alarm configuration scope

Although the BCM450 system provides a default mapping of alarms that are displayed in the Alarms table and that are sent as an SNMP trap, you may want to monitor additional alarms using either of these means, or you may want to reduce the number of alarms that are displayed in the Alarms table or sent via SNMP traps. You can specify how each alarm is handled, according to your business requirements.

You can specify the following settings for alarms:

- the maximum number of alarms to display in the Alarms Panel (from 50 to 400)
- whether to enable or disable SNMP traps for selected alarms; by default, the system sends all Critical and Major alarms as SNMP traps if you specify one or more trap destinations
- whether to display selected alarms in the Alarms table; by default all Critical, Major, Minor, and Warning alarms are displayed in the Alarms table
- whether to display selected alarms on the alarm set; by default, only core telephony Critical and Major alarms are sent to this set

You can also test a selected alarm. This allows you to test whether the LED or SNMP traps are functioning as expected. Testing an alarm generates an alarm in the system. Alarms generated using the Test Alarm feature are identified in the Alarms table by the words “Test Event” in the alarm Problem Description field.

For information about using SNMP to monitor the BCM450 system, see the *BCM450 Configuration—Telephony Guide* (NN40160-502).



---

# Using the BCM450 fault management system

---

This section describes how to manage alarms generated by the BCM450 system and administer alarm settings.

## Using the BCM450 fault management system navigation

- [Administering alarms \(page 19\)](#)
- [Using the alarm banner \(page 21\)](#)
- [Using the alarm set \(page 22\)](#)
- [Responding to LED indicators \(page 22\)](#)
- [Configuring alarm behaviour \(page 23\)](#)

## Administering alarms

This section contains information on the following topics:

- [Monitoring an alarm condition \(page 19\)](#)
- [Acknowledging an alarm \(page 20\)](#)
- [Clearing the alarm log \(page 21\)](#)

## Monitoring an alarm condition

Use the following procedure to monitor an alarm condition.

### Procedure steps

---

Step	Action
1	Click the <b>Administration</b> tab.
2	Open the <b>General</b> folder, and then click the <b>Alarms</b> task.
3	The <b>Alarms</b> page opens.
4	In the <b>Alarms Panel</b> table, select an alarm.
5	The <b>Alarm Details</b> pane displays below the <b>Alarms</b> table.

---

- 6 To change the order of columns in the Alarm table, select a column and drag it left or right to the desired location, and release it.
- 7 To view a column by ascending or descending order, click the column heading.
- 8 To sort columns, right-click a column heading.
- 9 The **Sort** dialog box opens.
- 10 Sort columns as required, and then click **OK**.
- 11 The columns in the **Alarms** table are sorted according to your specifications.

---

--End--

---

### Acknowledging an alarm

Use the following procedure to acknowledge an alarm.

#### Procedure steps

---

Step	Action
1	Click the <b>Administration</b> tab.
2	Open the <b>General</b> folder, and then click the <b>Alarms</b> task. The <b>Alarms</b> pane opens.
3	In the <b>Alarms</b> table, select the alarm you want to acknowledge. The <b>Alarm Details</b> pane is displayed below the <b>Alarms</b> table.
4	On the <b>Alarms Details</b> pane, click the <b>Acknowledge Alarm</b> button. A check box appears in the <b>Alarm Acked</b> column in the <b>Alarms</b> table for this alarm.

---

**Attention:** Acknowledging the alarm does not clear the alarm; it indicates only that you have noted it.

---

---

--End--

---

### Clearing the alarm log

Use the following procedure to clear the alarm log.

#### Procedure steps

---

Step	Action
1	Click the <b>Administration</b> tab.
2	Open the <b>General</b> folder, and then click the <b>Alarms</b> task. The <b>Alarms</b> pane opens.
3	On the <b>Alarms</b> pane, click the <b>Clear Alarm Log</b> button. The <b>Alarms</b> table is cleared. You will be able to see all new alarms only after the next alarm polling interval.

---

--End--

---

### Using the alarm banner

Use the alarm banner to view current alarm counts and recent alarm activity on the BCM450 system.

#### Including or omitting acknowledged alarms in the Alarm Banner

Use the following step to include or omit acknowledged alarms in the Alarm Banner.

#### Procedure steps

---

Step	Action
1	Select or clear the <b>Include Acked Alarms</b> check box in the Alarm Banner.

---

--End--

---

## Using the alarm set

Use the alarm set to monitor alarm activity without having a BCM450 Element Manager and a personal computer.

### Configuring the alarm set

Use the following steps to configure the alarm set.

#### Procedure steps

---

Step	Action
1	Click the <b>Configuration</b> tab.
2	Open the <b>Telephony</b> folder.
3	Open the <b>Global Settings</b> folder, and then click the <b>Feature settings</b> task. The <b>Feature Settings</b> page opens.
4	In the <b>Feature Settings</b> area, enter the DN of the telephone set that you want to use for the alarm set in the <b>Alarm Set</b> field.

---

--End--

---

### Clearing an alarm from the alarm set

Use the following step to clear an alarm from the alarm set.

#### Procedure steps

---

Step	Action
1	On the alarm set, press the <b>Clear</b> soft key. The alarm is cleared from the alarm set.

---

--End--

---

## Responding to LED indicators

Use the BCM450 Element Manager to reset the Status LEDs on the front panel of the BCM450 to a normal state.

### Reset the status LED

Use the following steps to reset the status LED.

---

### Procedure steps

---

Step	Action
1	Click the <b>Administration</b> tab.
2	Open the <b>General</b> folder, and then click the <b>Alarms</b> task. The <b>Alarms</b> pane opens
3	On the <b>Alarms</b> pane, click the <b>Reset LEDs</b> button.
4	The Status LED on the front panel of the BCM450 is reset from red to normal operation green.

---

--End--

---

## Configuring alarm behaviour

Configure alarm behaviour to specify the following settings for alarms:

- the maximum number of alarms to display in the Alarms Panel (from 50 to 400)
- whether to enable or disable SNMP traps for selected alarms; by default, all Critical and Major alarms are sent as SNMP traps if you have specified one or more trap destinations
- whether to display selected alarms in the Alarms table; by default all Critical, Major, Minor, and Warning alarms are displayed in the Alarms table
- whether to display selected alarms on the alarm set; by default, only core telephony Critical and Major alarms are sent to this set

### Enabling or disabling SNMP traps for alarms

Use the following procedure to enable or disable SNMP traps for alarms.

---

### Procedure steps

---

Step	Action
1	Click the <b>Administration</b> tab.
2	Open the <b>General</b> folder, and then click the <b>Alarm Settings</b> task.
3	In the <b>Alarm Settings</b> table, select an alarm.
4	In the <b>Enable SNMP Trap</b> column, select or clear the check box to enable or disable SNMP traps for the selected alarm. If you select the check box for a selected alarm, an SNMP trap will be generated if that particular alarm condition occurs.

---

--End--

---

### Enabling or disabling monitoring for selected alarms

Use the following procedure to enable or disable alarms.

#### Procedure steps

---

Step	Action
1	Click the <b>Administration</b> tab.
2	Open the <b>General</b> folder, and then click the <b>Alarm Settings</b> task. The <b>Alarm Settings</b> pane opens.
3	In the <b>Alarms Settings</b> table, select an alarm.
4	In the Enable GUI View column, select or clear the check box to enable or disable a view of the selected alarm in the Alarms Panel. If you clear the check box for a selected alarm, the alarm will not be displayed in the Alarms table if that particular alarm condition occurs in the system.

---

--End--

---

### Monitoring settings for the alarm set

Use the following procedure to monitor settings for the alarm set.

#### Procedure steps

---

Step	Action
1	Click the <b>Administration</b> tab.
2	Open the <b>General</b> folder, and then click the <b>Alarm Settings</b> task. The <b>Alarm Settings</b> pane opens.
3	In the <b>Alarms</b> table, select an alarm.
4	The <b>Enable Alarm Set</b> column indicates whether the alarm will display on the alarm set.

---

--End--

---



## Testing an alarm

Use the following procedure to test an alarm.

### Procedure steps

---

Step	Action
1	Click the <b>Administration</b> tab.
2	Open the <b>General</b> folder, and then click the <b>Alarm Settings</b> task. The <b>Alarm Settings</b> pane opens.
3	In the <b>Alarm Settings</b> table, select an alarm.
4	Click the <b>Test Alarm</b> button. In the Alarms table, "Test Event" is displayed in the alarm Problem Description field.

---

--End--

---



---

# Alarm Severity reference

---

This section contains information about Alarm Severities, default mapping of security levels, and Alarm graph colours in Element Manager.

## Navigation

- [Alarm Severities \(page 27\)](#)
- [Default mapping of severity levels \(page 27\)](#)
- [Alarm graph colours in Element Manager \(page 28\)](#)

## Alarm Severities

Alarm severities are as follows:

**Table 2 Alarm severities**

Alarm Severity	Description
Critical	Immediate corrective action is required due to conditions such as loss of service, loss of bandwidth, outage, loss of data, and/or functionality
Major	Urgent corrective action is required due to conditions such as pending loss of service, outage, loss of data, and/or functionality
Minor	Corrective action is required to prevent eventual service-affecting degeneration
Warning	Indicates the detection of a potential or impending service-affecting condition and that some diagnostic action is required
Information	Indicates audit-type information, such as configuration changes

## Default mapping of severity levels

Use the following table to view the default mapping of each severity level against the Alarms Panel, alarms set, LEDs, and SNMP.

**Table 3 Default mapping of severity levels**

Alarm Severity	Alarms Panel	LEDs	SNMP	Alarm Set (core telephony alarms only)
Critical	Yes	Yes	Yes	Yes
Major	Yes	Yes	Yes	Yes
Minor	Yes	No	No	No
Warning	Yes	No	No	No
Information	Yes	No	No	No

## Alarm graph colours in Element Manager

Use the following table to view alarm graph colours in Element Manager.

**Table 4 Alarm graph colours in Element Manager**

Color	Indicates
Green	There are no alarms of this severity, or there are alarms of this severity but the count has decreased since the last polling interval.
Yellow	There are alarms of this severity, but they are older than at least 1 polling interval.
Red	A new alarm has occurred since the last polling interval.

---

# System metrics monitoring

---

You can use the Element Manager to view detailed information about the performance of the BCM450 and about the performance of system resources. This chapter provides procedures for monitoring quality of service (QoS) and other system metrics.

Using the Element Manager, you can monitor overall system performance and other performance-related information.

You monitor system metrics using the following tools:

- UPS Status
- NTP Metrics

This section contains information on the following topics:

- [QoS Monitoring \(page 29\)](#)
- [UPS metrics \(page 33\)](#)
- [NTP metrics \(page 34\)](#)

## QoS Monitoring

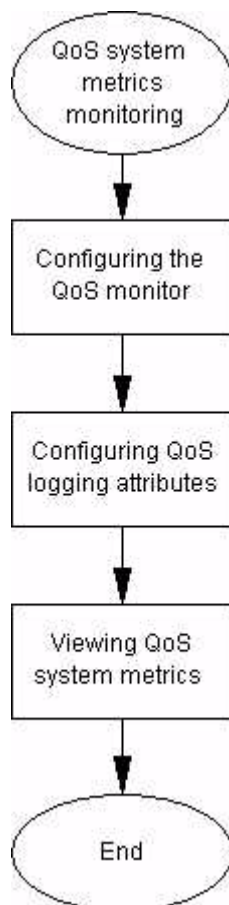
QoS Monitor monitors the quality of service (QoS) of IP trunk services. The tool periodically monitors the delay and packet-loss of IP networks between two peer gateways. The main objective of the QoS Monitor is to allow new IP telephony calls to fall back to the PSTN if the voice quality of the IP network falls below the specified transmit threshold.

For information about setting the transmit threshold, see *Nortel Business Communications Manager 450 1.0 Configuration—Telephony (NN40160-502)*. You can set the threshold in the Element Manager in the Telephony Resources panel.

## QoS system metrics monitoring procedures

This task flow shows you the sequence of tasks you perform to monitor QoS statistics on the BCM450 system. To link to any procedures, click on [QoS system metrics monitoring procedures navigation \(page 30\)](#).

**Figure 2 QoS system metrics monitoring procedures**



**QoS system metrics monitoring procedures navigation**

- [Configuring the QoS monitor \(page 31\)](#)
- [Configuring QoS logging attributes \(page 31\)](#)
- [Viewing QoS logs \(page 32\)](#)

## Configuring the QoS monitor

You configure the QoS Monitor using the QoS Monitor panel on the Administration tab. You can configure the following:

- the monitoring mode
- logging parameters

### Procedure steps

Step	Action
1	Click the <b>Administration</b> tab.
2	In the Navigation tree, click <b>System Metrics &gt;QoS Monitor</b> .
3	From the <b>Monitoring Mode</b> drop-down menu, select a monitoring mode.

--End--

**Table 5 Variable definitions**

Variable	Value
Disabled	—
Enabled in Link-Monitor mode	Continuously test the connection between the BCM450 and remote endpoints.
Enabled in QoS-Monitor mode	Select this option if you want to calculate MOS values for each endpoint, determine whether the connection has fallen below a specific threshold, send MOS scores to FCAPS applications, and create a log history of the MOS scores.

## Configuring QoS logging attributes

Configure the logging attributes to set the size and frequency of QoS logs.

### Procedure steps

Step	Action
1	Click the <b>Administration</b> tab.
2	In the Navigation tree, click <b>System Metrics&gt;QoS Monitor</b> .
3	In the Logging area, select or deselect the <b>Enable Logging</b> checkbox.
4	In the <b>Maximum log file size</b> field, type the value of the maximum log size allowed.

- 5 In the **Logging Frequency** field, type the value of the interval between logs.  
*After the interval you specified, the QoS system metrics appear in the Mean Opinion Scores table.*

---

--End--

---

**Table 6 Variable definitions**

Variable	Value
Enable Logging	Enable the check box if you want to enable the logging of MOS scores.
Maximum log file size	Enter a value for the maximum size of the log file, from 1 to 10240 kilobytes (KB). The default is 10 KB.
Logging Frequency	Enter the time interval between each MOS log: 1 to 1440 minutes. The default is 1 minutes.

### Viewing QoS logs

The Mean Opinion Scores table displays the current network quality described as a Mean Opinion Score (MOS) for each IP destination. You can view the MOS mapping. Unlike the BCM 3.x where both transmit and receive values were reported, the QoS Monitor collects only the transmit values.

### Procedure steps

---

Step	Action
1	Click the <b>Administration</b> tab.
2	In the Navigation tree, click <b>System Metrics&gt;QoS Monitor</b> . <i>The QoS system metrics appear in the Mean Opinion Scores table.</i>
3	To update the MOS table with the most current values, select <b>View &gt; Refresh</b> , press <b>F5</b> , or select the <b>Refresh</b> icon from the toolbar.

---

--End--

---

**Table 7 Variable definitions**

Variable	Value
Name	Displays the name of the Remote Gateway.
IP Address	Displays the IP address of the Remote Gateway.
QoS Indicator	Displays a text description of the current MOS value. The MOS values can be Poor, Fair, Good or Excellent.



Table 7 Variable definitions

Variable	Value
G.711	Displays the current MOS value calculated when using a G.711 aLaw codec to transmit VoIP packets to this Remote Gateway.  The MOS can be a value from 0.00 to 5.00, where 0.00 is the worst score (Poor) and 5.00 is best score (Excellent).
G.723-5.3kbit/s	Displays the current MOS value calculated when using a G.723 5.3 kbit/s codec to transmit VoIP packets to this Remote Gateway.  The MOS can be a value from 0.00 to 5.00, where 0.00 is the worst score (Poor) and 5.00 is best score (Excellent).
G.723-6.3kbit/s	Displays the current MOS value calculated when using a G.723 6.3 kbit/s codec to transmit VoIP packets to this Remote Gateway.  The MOS can be a value from 0.00 to 5.00, where 0.00 is the worst score (Poor) and 5.00 is best score (Excellent).
G.729	Displays the current MOS value calculated when using a G.729 codec to transmit VoIP packets to this Remote Gateway.  The MOS can be a value from 0.00 to 5.00, where 0.00 is the worst score (Poor) and 5.00 is best score (Excellent).
G.729A	Displays the current MOS value calculated when using a G.729A codec to transmit VoIP packets to this remote Gateway.  The MOS can be a value from 0.00 to 5.00, where 0.00 is the worst score (Poor) and 5.00 is best score (Excellent).

## UPS metrics

The BCM450 can support an Uninterruptible Power Supply (UPS) device to ensure continuous operation during power interruption and failure conditions. The UPS feature provides power source monitoring and battery backup so that critical system functionality required to maintain and provide warning time to either correct the problem or to activate a contingency plan for impacted services is possible. UPS is described in *Nortel Business Communications Manager 450 1,0 Installation — System (NN40160-301)* and *BCM450 Installation Checklist and Quick Start Guide (NN40160-300)*.

The UPS connects and communicates with the BCM450 through USB. Enable the UPS feature by plugging the UPS USB cable into the BCM450 USB connector before you power up the BCM450. The UPS must be present during the boot up process for the BCM450 to function.

The UPS Status panel tracks occurrences of alarms pertaining to UPS operation. These alarms are also sequentially viewable in the Alarm panel. The metrics correspond to alarms in the BCM450 and appear in the alarm panel as well.

### Accessing the UPS status

Complete this procedure to verify the status of the UPS before you boot up the BCM450 system.

#### Procedure steps

---

Step	Action
1	Click the <b>Administration</b> tab.
2	In the Navigation tree, click <b>System Metrics &gt;UPS Metrics &gt; Status</b> tab. <i>The status of the UPS appears. The UPS Status panel confirms that a UPS is connected including model and serial number, its current status, and provides a read out of the current values. Additionally, an indication is given whether the value is within the normal range or not.</i>
3	To check the metrics of the UPS, click the <b>Metrics</b> tab. <i>The metrics information appears in the panel.</i>

---

--End--

---

### NTP metrics

Using Network Time Protocol (NTP), you can configure the time on the BCM450 indirectly from a single time server. NTP is a network protocol designed to synchronize the clocks of computers over an IP network. The NTP Metrics provide an overview of the integrity of the NTP time source. If the BCM450 clock control has not been configured to use NTP (Configuration>System>Date & Time), then the NTP Metrics panel displays no data.

## Accessing the NTP metrics

Complete this procedure to view NTP metrics.

### Procedure steps

Step	Action
------	--------

- |   |   |
|---|---|
| 1 | Click the <b>Administration</b> tab.  |
| 2 | In the Navigation tree, click <b>System Metrics&gt;NTP Metrics</b> .<br><i>The NTP metrics appear in the panel.</i> |

--End--

**Table 8 Variable definitions**

Variable	Value
Last Synchronized	When the last synchronization occurred.
Minimum time difference (s)	The minimum time change that occurred since NTP was running.
Maximum time difference (s)	The maximum time difference that occurred since NTP was running.
Last Synchronization Status	The results of the last synchronization: successful or unsuccessful. If unsuccessful the reason for the failure is given: failed to contact, or failed security check. A status of Not Running indicates that NTP is not configured.



---

# Telephony metrics monitoring

---

You can use the Element Manager to view detailed information about the performance of telephony resources on the BCM450 system.

The Telephony Metrics folder allows you to track different aspects of Telephony services.

This section contains information on the following topics:

- [Proactive Voice Quality Management \(page 37\)](#)
- [Activity Reporter Basic \(page 44\)](#)
- [Trunk module metrics \(page 46\)](#)
- [Trunk module CSU statistics \(page 48\)](#)
- [CbC limit metrics \(page 54\)](#)
- [Hunt group metrics \(page 56\)](#)
- [PSTN Fallback metrics \(page 58\)](#)

## Proactive Voice Quality Management

Use Proactive Voice Quality Management (PVQM) metrics to monitor the quality of VoIP calls. You can also use the PVQM metrics to diagnose infrastructure problems in your network.

PVQM is fully supported on Phase 2 IP sets. Phase 1 IP sets support only the following PVQM metrics: packet loss, inter arrival jitter, and round trip delay. The following table lists the IP Phones that support PVQM.

**Table 9 PVQM set support**

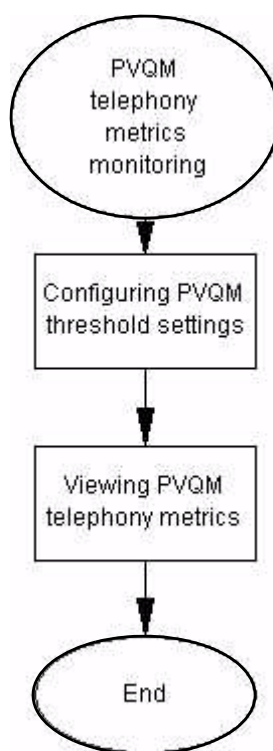
IP Set Type	Description
IP Phone 2001	Phase 2 firmware
IP Phone 2002	Phase 1 and Phase 2 firmware
IP Phone 2004	Phase 1 and Phase 2 firmware
IP Phone 2050 v2	PC-based soft client

**Table 9 PVQM set support**

IP Set Type	Description
IP Phone 2007	Phase 2 firmware
IP Phone 1120E	Phase 2 firmware
IP Phone 1140E	Phase 2 firmware

### PVQM telephony metrics monitoring procedures

This task flow shows you the sequence of tasks you perform to configure and monitor PVQM telephony metrics on the BCM450 system. To link to any procedures, click on [PVQM telephony metrics monitoring procedures navigation \(page 38\)](#).

**Figure 3 PVQM telephony metrics monitoring procedures**

### PVQM telephony metrics monitoring procedures navigation

- [Setting the PVQM threshold settings \(page 39\)](#)
- [Viewing PVQM telephony metrics \(page 43\)](#)

## Setting the PVQM threshold settings

You can use PVQM to configure and report threshold violations for the following voice quality metrics:

- packet loss—packets lost in transit due to errors or network failures
- inter arrival jitter—the variable delay on a packet as it traverses a network
- round trip delay
- listening R factor—the transmission quality as experienced by the user; this metric reflects the segment of the call that is carried over the RTP session

There are two thresholds for PVQM metrics: Warning, and Unacceptable. A violation of the Warning threshold indicates that the voice quality is reduced but is still within an acceptable range. A violation of the Unacceptable threshold indicates a severe degradation in voice quality.

If an alarm is generated to report a threshold violation, additional information is included in the alarm to indicate the source of the alarm and provide other troubleshooting information. [Table 10 PVQM Alarms \(page 39\)](#) lists the abbreviations used in the alarm text to present this additional information.

**Table 10 PVQM Alarms**

Abbreviation	Attribute	Value	Description
cT	codec type	alphanumeric	Vocoder type used on this call
eT	endpoint type	S or D	S indicates softclient D indicates desktop
nLR	network loss rate	percentage, scaled by 256 (e.g. 354 = 1.4%)	Rate of network packet loss
dR	average discard rate	percentage, scaled by 256	Average rate of discards due to jitter
bD	burst loss density	percentage, scaled by 256	Density of lost and discarded packets during burst periods
bL	burst length	milliseconds	Average length of bursts
gD	gap loss density	percentage, scaled by 256	Density of lost and discarded packets during gap periods
gL	average length of gap	milliseconds	average length of gap
eSD	end system delay	milliseconds	Average end system delay on the call
aNL	noise level	dBm	Measured received silent period noise level

**Table 10 PVQM Alarms**

Abbreviation	Attribute	Value	Description
aSP	average signal level	dBm	Measured received signal level during talk spurts
rTT	local round trip time average	1/65536 of a second	Average round trip time on the call

---

**Procedure steps**

---

- | Step | Action   |
|------|--|
| 1    | Click the <b>Administration</b> tab.   |
| 2    | In the Navigation tree, click <b>Telephony Metrics&gt;PVQM&gt;Threshold settings</b> .<br><i>The Proactive Voice Quality Monitoring panel appears.</i> |
| 3    | In the <b>Threshold settings</b> table, select the metric you want to configure.   |
| 4    | In the <b>Warning (desktop)</b> column, double click the value and type the threshold value you want to set.   |
| 5    | In the <b>Unacceptable (desktop)</b> column, double click the value and type the threshold value you want to set.                                      |
| 6    | In the <b>Warning (softclient)</b> column, double click the value and type the threshold value you want to set.  |
| 7    | In the <b>Unacceptable (softclient)</b> column, double click the value and type the threshold value you want to set.                                   |
| 8    | In the <b>Polling interval(s)</b> field, type the interval at which you want the metrics to be polled.   |

---

--End--

---



## Variable definitions

Variable	Value
Metric	<p>Contains the following PVQM metrics you can monitor:</p> <ul style="list-style-type: none"> <li>• Packet Loss Rate: The fraction of RTP data packets from the source lost since the beginning of the call, expressed as a percentage.</li> <li>• Inter-arrival Jitter : The inter-arrival time of incoming RTP packets, as defined in RFC 1889. Expressed in milliseconds.</li> <li>• RTCP Round Trip Delay: The round trip time of incoming RTP packets, as defined in RFC 1889. Measured in milliseconds.</li> <li>• Listening R Factor: A scale from 0 (lowest quality) to 100 (highest quality) according to ITU-T G.107.</li> </ul>
Warning (desktop)	<p>The number of warnings you can receive for a desktop phone model. The value ranges and default thresholds are as follows:</p> <ul style="list-style-type: none"> <li>• Packet Loss Rate: The value range for this metric is 0 to 100. The default value for warning thresholds is 1%.</li> <li>• Inter-arrival Jitter : The value range for this metric is 0 to 1000. The default value for warning thresholds is 50 ms.</li> <li>• RTCP Round Trip Delay: The value range for this metric is 0 to 1000. The default value for warning thresholds is 300 ms.</li> <li>• Listening R Factor: The value range for this metric is 0 to 100. The default value for warning thresholds is 65.</li> </ul>

Variable	Value
Unacceptable (desktop)	<p>The number of unacceptable errors you can receive for a desktop phone model. The value ranges and default thresholds are as follows:</p> <ul style="list-style-type: none"> <li>• Packet Loss Rate: The value range for this metric is 0 to 100. The default value for unacceptable thresholds is 5%.</li> <li>• Inter-arrival Jitter : The value range for this metric is 0 to 1000. The default value for unacceptable thresholds is 500 ms.</li> <li>• RTCP Round Trip Delay: TThe value range for this metric is 0 to 1000. The default value for unacceptable thresholds is 500 ms.</li> <li>• Listening R Factor: The value range for this metric is 0 to 100. There is no default value for unacceptable thresholds.</li> </ul>
Warning (softclient)	<p>The number of warnings you can receive for a softclient phone model. The value ranges and default thresholds are as follows:</p> <ul style="list-style-type: none"> <li>• Packet Loss Rate: The value range for this metric is 0 to 100. The default value for warning thresholds is 1%.</li> <li>• Inter-arrival Jitter : The value range for this metric is 0 to 1000. The default value for warning thresholds is 50 ms.</li> <li>• RTCP Round Trip Delay: TThe value range for this metric is 0 to 1000. The default value for warning thresholds is 300 ms.</li> <li>• Listening R Factor: The value range for this metric is 0 to 100. The default value for warning thresholds is 65.</li> </ul>

Variable	Value
Unacceptable (softclient)	<p>The number of unacceptable errors you can receive for a softclient phone model. The value ranges and default thresholds are as follows:</p> <ul style="list-style-type: none"> <li>• Packet Loss Rate: The value range for this metric is 0 to 100. The default value for unacceptable thresholds is 5%.</li> <li>• Inter-arrival Jitter : The value range for this metric is 0 to 1000. The default value for unacceptable thresholds is 500 ms.</li> <li>• RTCP Round Trip Delay: TThe value range for this metric is 0 to 1000. The default value for unacceptable thresholds is 500 ms.</li> <li>• Listening R Factor: The value range for this metric is 0 to 100. There is no default value for unacceptable thresholds.</li> </ul>
Polling interval(s)	<p>The interval at which the metrics are polled. The value for this field is XXXXX. The default value is XXXXX.</p>
<p><b>Attention:</b> The term “desktop” indicates IP sets that are desktop models. The term “soft client” indicates IP sets that are software applications, such as the 2050 and the 2050MVC. Because desktop IP sets can provide better voice quality than software-based IP sets, you can specify different threshold levels for each type of IP set.</p>	

### Viewing PVQM telephony metrics

Use this procedure to view PVQM metrics.

#### Procedure steps

Step	Action
1	Click the <b>Administration</b> tab.
2	In the Navigation tree, click <b>Telephony Metrics &gt;PVQM &gt;Metrics</b> . <i>The PVQM metrics panel appears.</i>
3	Click a column heading to sort the metrics by a particular value.

--End--

**Variable definitions**

Variable	Value
Number of connections	Displays the total number of connections by IP sets on the system since the last reset. This count includes non-interactive features such as dial tones, call progress tones, and music on hold.
Last rest	Displays the time of the last reset.
Most recent date and time	Displays the time of the most recent threshold violation.
Most recent DN	Displays the DN of the most recent threshold violation.
Count (desktop)	Displays the number of times a desktop client violated a threshold.
Count (softclient)	Displays the number of times a soft client violated a threshold.
MTBV (desktop)	Displays the mean time between threshold violations of a particular metric for desktop clients (measured in seconds).
MTBV (soft client)	Displays the mean time between threshold violations of a particular metric for soft clients (measured in seconds).
Reset metrics	Click this button to clear out the metrics table. The Last reset time displays the current date and time.

**Activity Reporter Basic**

This section contains information on the following topics:

- [Enabling Activity Reporter Basic \(page 44\)](#)
- [Disabling Activity Reporter Basic \(page 45\)](#)

**Enabling Activity Reporter Basic**

Activity Reporter Basic allows you to monitor the performance of the BCM. You can use the Activity Reporter Basic to generate the following reports:

- telephone call activity
- custom call routing activity
- voice mail receive statistics
- hunt group performance

When you enable Activity Reporter Basic, the BCM automatically generates reports and updates them each night. The reports reflect the performance of the BCM during the past four days. The panel displays the date and time of the most recent report.

---

### Procedure steps

---

Step	Action
1	Select <b>Administration &gt;Telephony Metrics &gt; Activity Reporter Basic</b> . <i>The Activity Reporter Basic panel appears.</i>
2	In the Activity Reporter Basic panel, select the <b>Enable daily data collection</b> checkbox to activate Activity Reporter Basic.
3	From the <b>Collection time</b> drop-down menu, select a time to generate daily reports.

---

--End--

---

### Variable definitions

Variable	Value
Enable daily data collection	Select or deselect the check box to enable Activity Reporter Basic.
Collection Time	Set the time at which the daily reports are generated. The default time is set at 12:30 am.
Most recent data collection	Displays a timestamp of the time at which data was last collected.

### Disabling Activity Reporter Basic

When you disable Activity Reporter Basic, the BCM does not generate performance reports .

---

### Procedure steps

---

Step	Action
1	Select <b>Administration &gt; Telephony Metrics &gt; Activity Reporter Basic</b> . <i>The Activity Reporter Basic panel appears.</i>
2	In the Activity Reporter Basic panel, deselect the <b>Enable daily data collection</b> checkbox to deactivate Activity Reporter Basic.

---

--End--

---

### Variable definitions

Variable	Value
Enable daily data collection	Deselect the check box to disable Activity Reporter Basic.

### Trunk module metrics

This section contains information on the following topics:

- [Viewing the trunk module status \(page 46\)](#)
- [Viewing performance history information \(page 46\)](#)
- [Viewing D-channel information \(page 47\)](#)
- [Disabling or enabling a B-channel setting \(page 47\)](#)
- [Provisioning a PRI B-channel \(page 48\)](#)

### Viewing the trunk module status

View the trunk module status to isolate malfunctioning parts of your BCM450 system. In addition, you can use the trunk module selection to disable and enable modules and devices.

### Procedure steps

---

Step	Action
1	Select <b>Administration &gt; Telephony Metrics &gt; Trunk Module Metrics</b> . The window displays the locations for the modules connected to the system.
2	Select the module that you want to view.
3	Click <b>Start Loopback Test</b> to start the network test without having to remove the module.
4	Select a loopback type from the list.
5	Click <b>Stop Loopback Test</b> when done the test of the network.

---

--End--

---

### Viewing performance history information

The Performance History tab displays the performance information over 15-minute intervals collected in the past 24 hours. The performance information collected includes the number of errored seconds, severely errored seconds, and unavailable seconds over each 15-minute interval.

---

### Procedure steps

Step	Action
1	Select <b>Administration &gt; Telephony Metrics &gt; Trunk Module Metrics</b> .
2	Click the <b>Performance History</b> tab to view metrics information.

---

--End--

---

### Viewing D-channel information

The D-channel tab displays trunk module metrics for the D-channel.

#### Prerequisites

- You must have a BRI trunk module configured on the BCM450 system.

### Procedure steps

Step	Action
1	Select <b>Administration &gt; Telephony Metrics &gt; Trunk Module Metrics</b> .
2	Select the BRI module.
3	Click the <b>D-channel</b> tab to view metrics information.

---

--End--

---

### Disabling or enabling a B-channel setting

If you need to isolate a problem, you can turn off individual port channels, rather than the entire module.

### Procedure steps

Step	Action
1	Select <b>Administration &gt; Telephony Metrics &gt; Trunk Module Metrics</b> . The Trunk Modules window displays the MBM location, type, state, and Loopback test.
2	Click the heading of the bus you want to view.
3	Click the tab in the lower menu marked B-channels.
4	Click the B-channel you want to enable or disable (B1 or B2).
5	Select <b>Enable</b> or <b>Disable</b> .

If you are disabling the channel, you are prompted by a dialog box to confirm your action. The State box indicates the mode of operation for the port. If the port is enabled, this box is blank unless a device is physically connected.

---

--End--

---

### Provisioning a PRI B-channel

When you purchase PRI from your service provider, you can request the number of B-channels that are allocated for you to use. For example, you can use 12 B-channels. If you do not have all of the PRI B channels, disable all the B-channels that you do not need.

#### Prerequisites

- Nortel recommends that the number of lines you deprovision on a DTM (configured as PRI) be the same as the number of B-channels that you disable. For example, if the DTM is on Expansion 1, when you disable B-channels 13 to 23, you should deprovision lines 77 to 87.

#### Procedure steps

---

Step	Action
1	Select <b>Administration &gt; Telephony Metrics &gt; Trunk Module Metrics</b> .
2	Choose a module.
3	Click <b>B-channels</b> . A list of the B-channels on this module appears.
4	Click a channel, for example, B 01. The display shows the status of the PRI channel.
5	Click the <b>Enable</b> or <b>Disable</b> button to change the setting for the channel.

---

--End--

---

### Trunk module CSU statistics

Each trunk module has an internal channel service unit (CSU). When enabled, the internal CSU monitors the quality of the received T1 signal and provides performance statistics, alarm statistics, and diagnostic information.

Trunk modules must be individually programmed to establish parameters for collecting and measuring transmission performance statistics by the CSU.



The system accumulates three performance parameters:

- errored seconds (ES)
- severely errored seconds (SES)
- unavailable seconds (UAS)

These parameters are defined according to TIA-547A. Errored seconds are enhanced to include control slip (CS) events. Only near-end performance data is recorded.

The internal CSU continuously monitors the received signal and detects four types of transmission defects:

- any active carrier failure alarms (CFA), such as loss of signal (LOS), out of frame (OOF), alarm indication signal (AIS), and remote alarm indication (RAI)
- the number of bipolar violations that occurred in the last minute
- any defects that occurred in the last minute, such as loss of signal (LOS), out of frame (OOF), and alarm indication signal (AIS)
- the number of milliseconds of short-term alarms in the last minute, such as loss of signal (LOS), out of frame (OOF), alarm indication signal (AIS), and remote alarm indication (RAI).

A short term alarm is declared when the detected defects persist for tens of milliseconds. A carrier failure alarm (CFA) is a duration of carrier system outage.

The criteria for declaring and clearing the alarms is selectable to meet those in TIA-547A or TR64211. You can also view Carrier Failure Alarms as Core Telephony Alarms in the Alarm Viewer.

### **BCM450 trunk module CSU statistics navigation**

- [Enabling the internal CSU \(page 50\)](#)
- [Checking the performance statistics \(page 50\)](#)
- [Checking the CSU alarms \(page 51\)](#)
- [Checking carrier failure alarms \(page 51\)](#)
- [Checking bipolar violations \(page 52\)](#)
- [Checking short-term alarms \(page 53\)](#)
- [Checking defects \(page 53\)](#)
- [Viewing CSU alarm history \(page 54\)](#)

### Enabling the internal CSU

Enable the internal CSU to gather performance statistics for your T1 lines or PRI with public interface.

#### Procedure steps

---

Step	Action
1	Select <b>Configuration &gt; Resources &gt; Telephony Resources</b> .
2	Select the appropriate module.
3	Click the <b>Trunk Module Parameters</b> tab.
4	In the T1 Parameters section, select the <b>Internal CSU</b> check box to enable the Internal CSU.

---

--End--

---

### Checking the performance statistics

Check the performance statistics to determine if the system detects errors or alarms within the selected period.

#### Procedure steps

---

Step	Action
1	Select <b>Administration &gt; Telephony Metrics &gt; Trunk Module Metrics</b> .
2	Select the appropriate module.
3	Click the <b>Performance</b> tab.  The Current interval displays the duration of the current 15-minute interval of the selected card, the number of errored seconds (ES), the number of severely errored seconds (SES), and the number of unavailable time seconds (UAS).
4	Click the 24-hour summary heading for an overall summary of the previous 24 hours.  The Number of intervals, Errored Seconds, Severely Errored Seconds, Unavailable Seconds appear in the summary.
5	Click <b>Reset Statistics</b> to reset new settings.  The system displays a message indicating that this will remove all of the statistics.

- 
- 6 Click **OK** to erase all the current statistics and begin collecting statistics again.
- 

--End--

---

### Checking the CSU alarms

Check the CSU alarms to view the active loss of signal (LOS), out of frame (OOF), remote alarm indicator (RAI), or alarm indication signal (AIS) alarms.

#### Procedure steps

---

Step	Action
1	Select <b>Administration &gt; Telephony Metrics &gt; Trunk Module Metrics</b> .
2	Select a module.
3	Click the <b>CSU Alarms</b> tab.  The display shows all the active alarms of the types LOS (loss of signal), OOF (out of Frame), RAI (Remote alarm indicator), or AIS (Alarm indication signal).

---

--End--

---

### Checking carrier failure alarms

Check carrier failure alarms to view a history of alarms for a module. CFA types reported by the BCM450 can be mapped to CFAs defined in TIA-547A and TR62411 as shown in the table below.

#### Procedure steps

---

Step	Action
1	Select <b>Administration &gt; Telephony Metrics &gt; Trunk Module Metrics</b> .
2	Select a module.
3	Click the <b>CSU Alarm History</b> tab.  The display shows LOS (loss of signal), OOF (out of Frame), AIS (Alarm indication signal), and RAI (Remote alarm indicator).
4	Select the type of alarm you wish to view.

- 5 Select a time period.  
The display shows the start time of the period.

---

--End--

---

### Variable definitions

Table 11

Business Communications Manager	TIA-547A	TR62411
LOS CFA	RED CFA	RED CFA
OOF CFA	RED CFA	RED CFA
AIS CFA	RED CFA	AIS CFA
RAI CFA	YELLOW CFA	YELLOW CFA

### Checking bipolar violations

Check bipolar violations to view the number of bipolar violations occurring within the defined time period.

### Procedure steps

---

- | Step | Action   |
|------|--|
| 1    | Select <b>Administration &gt; Telephony Metrics &gt; Trunk Module Metrics</b> .  |
| 2    | Select a module.   |
| 3    | Click the <b>CSU Alarms</b> tab.<br><br>The display shows the number of bipolar violations that occurred in the last minute. |
- 

--End--

---

### Checking short-term alarms

Check short-term alarms to view the number of alarms within the last minute.

#### Procedure steps

---

Step	Action
------	--------

---

1	Select <b>Administration &gt; Telephony Metrics &gt; Trunk Module Metrics</b> .
---	---

2	Select a module.
---	------------------

3	Click the <b>CSU Alarms</b> tab.
---	----------------------------------

The display shows the short term alarms and the number of milliseconds (not necessarily contiguous) that were active in the last minute.

---

--End--

---

### Checking defects

Check defects to view the first type of defect in the last minute.

#### Procedure steps

---

Step	Action
------	--------

---

1	Select <b>Administration &gt; Telephony Metrics &gt; Trunk Module Metrics</b> .
---	---

2	Select a module.
---	------------------

3	Click the <b>CSU Alarms</b> tab.
---	----------------------------------

The display shows the first type of defect and the number of milliseconds (not necessarily contiguous) the hardware reported in the last minute.

---

--End--

---

### Viewing CSU alarm history

View CSU alarm history to view all occurrences of a specific alarm.

#### Procedure steps

---

Step	Action
1	Select <b>Administration &gt; Telephony Metrics &gt; Trunk Module Metrics</b> .
2	Select a module.
3	Click the <b>CSU Alarm History</b> tab. The display shows all the alarms.
4	To view a specific alarm, click the alarm name. The display shows all the occurrences of that alarm.

---

--End--

---

### CbC limit metrics

This section contains information on the following topics:

- [Accessing CbC limit metrics \(page 54\)](#)
- [Clearing CbC limit metrics \(page 56\)](#)

#### Accessing CbC limit metrics

Call-by-call service (CbC) on public PRI protocol (NI-2) allows a PBX to use channels more effectively by expanding or contracting the number of channels available to different call types such as INWATS, OUTWATS, Foreign Exchange (FX), and tie lines.

The call-by-call service is a method of offering and receiving services to Customer Premises Equipment (CPE) on ISDN PRI without the use of dedicated circuits (i.e. interface or B-channels). The Call-By-Call service conveys signaling information over an ISDN Primary Rate Interface (PRI) that indicates, on a per-call basis, the specific service type required to complete the call.

Although PRI-MCDN and IP trunks do not have multiple call types, CbC limits can be used on these trunks to limit the number of incoming or outgoing trunks that may be in use simultaneously.

When the CbC the feature is configured, use the CbC Limit metrics panel to monitor denied call activity for each service on each line pool.

PRI lines that support call-by-call services have maximum and minimum call limits for each service. Use this panel to view reports for the services and to assess the capacity of the PRI call services on your system. These limits are set as part of the numbering plan programming.

### Procedure steps

Step	Action
1	Click the <b>Administration</b> tab.
2	In the Navigation tree, click <b>Telephony Metrics &gt;CbC Limit Metrics</b> .
3	In the <b>Call by CallLimit Metrics</b> table, select the line pool for which you want to view CbC traffic.

*The denied call details for each type of service supported by the line pool appears in the Details for Pool table.*

--End--

### Variable definitions

Variable	Value
Line Pool	The pool of lines that call-by-call limits are applied to.
Service Type	The type of service that the limits apply to.
INCOMING due to Outgoing Min.	The number of incoming calls that have been blocked due to the call-by-call limits.
due to Incoming Max.	The number of incoming calls that have been blocked due to call-by-call limits.
OUTGOING due to Incoming Min.	The number of outgoing calls that have been blocked due to the call-by-call limits.
due to Outgoing Max.	The number of outgoing calls that have been blocked due to the call-by-call limits.

### Clearing CbC limit metrics

Use this procedure to clear the Details for Pool table of the current CbC limit metrics, and start a new monitoring period.

#### Procedure steps

---

Step	Action
1	Click the <b>Administration</b> tab.
2	In the Navigation tree, click <b>Telephony Metrics&gt;CbC Limit Metrics</b> .
3	In the <b>Call by Call Metrics</b> table, select the line pool for which you want to view CbC traffic.  <i>The denied call details for each type of service supported by the line pool appears in the Details for Pool table.</i>
4	Select one of the calls in the <b>Calls denied because CbC limits were exceeded</b> list.
5	Click the <b>Reset Metrics</b> button.

---

--End--

---

### Hunt group metrics

This section contains information on the following topics:

- [Accessing Hunt Group metrics \(page 56\)](#)
- [Resetting the Hunt Group metrics \(page 58\)](#)

#### Accessing Hunt Group metrics

Hunt groups provide a service where incoming calls ring on a targeted group of telephones called a Hunt group. When you designate a Hunt group, you define the group as a unique Directory Number (DN). This DN receives and distributes calls to the telephones assigned to the group.

You can include Hunt Group hourly metrics files with the CDR data files when they are transferred to the central server. For more information on configuring this option, refer to the *Call Detail Recording System Configuration Guide* (NN40020-605).

Access the Hunt Group metrics to evaluate total call processing by hunt group member.



---

## Procedure steps

Step	Action
1	Click the <b>Administration</b> tab.
2	In the Navigation tree, click <b>Telephony Metrics&gt;Hunt Group Metrics</b> . <i>The Hunt Groups table appears.</i>
3	In the <b>Hunt Groups</b> table, select the Hunt Group for which you want to see metrics. <i>The Details for Hunt Group table appears.</i>

---

--End--

---

## Variable definitions

Variable	Value
Hunt Group	Name of the hunt group.
Name	Name entered on the DN record.
Total calls	Total number of calls.
Answered: Total	Total number of answered calls.
Answered: Avg%	Average number of answered calls.
Answered: Avg time(s)	Average answer time.
Abandoned: Total	Total number of abandoned calls.
Abandoned: Avg%	Average number of abandoned calls.
Busy: Total	Total number of busy calls.
Busy: Avg%	Average number of busy calls
Overflow: Total	Total number of overflow calls.
Overflow: Avg%	Average number of overflow calls.
Time in Queue	Time in queue.
Last Reset time	Time and date format depends on the country profile of the system.

### Resetting the Hunt Group metrics

Use this procedure to reset the Hunt Group metrics.

#### Procedure steps

---

Step	Action
1	Click the <b>Administration</b> tab.
2	In the Navigation tree, click <b>Telephony Metrics&gt;Hunt Group Metrics</b> . <i>The Hunt Groups table appears.</i>
3	In the <b>Hunt Groups</b> table, select the Hunt Group for which you want to reset the metrics. <i>The Details for Hunt Group table appears.</i>
4	Click the <b>Reset</b> button.

---

--End--

---

### PSTN Fallback metrics

This section contains information on the following topics:

- [Accessing PSTN Fallback metrics \(page 58\)](#)
- [Resetting PSTN Fallback metrics \(page 59\)](#)

#### Accessing PSTN Fallback metrics

When trunks are out of service, traffic can be switched to PSTN fallback lines. Use this procedure to view how many fallback attempts and fallback failures occur within a specific period using the PSTN Fallback Metrics panel.

#### Procedure steps

---

Step	Action
1	Click the <b>Administration</b> tab.
2	In the Navigation tree, click <b>Telephony Metrics&gt;PSTN Fallback Metrics</b> . <i>The PSTN Fallback Metrics panel appears with the metrics displayed.</i>

---

--End--

---

---

## Variable definitions

Variable	Definition
Last reset time	The date and time the metrics table was last reset.
Fallback requests	The number of calls unable to route through the preferred trunk.
Fallback failures	The number of calls unable to route though the fallback trunk.

## Resetting PSTN Fallback metrics

Use this procedure to clear the PSTN Fallback Metrics panel.

---

Step	Action
1	Click the <b>Administration</b> tab.
2	In the Navigation tree, click <b>Telephony Metrics&gt;PSTN Fallback Metrics</b> . <i>The PSTN Fallback Metrics panel appears with the metrics displayed.</i>
3	Click the <b>Reset</b> button.

---

--End--

---



---

# System LEDs reference

---

This section provides information about the main unit LED status during normal operation, startup, and reboot.

## Navigation

- [System status monitor LEDs \(page 61\)](#)

## System status monitor LEDs

The BCM450 system status LEDs on the main unit provide information about the status of the BCM450 system. Use these LEDs to determine if the system is functioning properly and if the system generates an alarm.

**Table 12 System status LEDs states and descriptions**

Power	Status	Description
<b>Start-up sequence</b>		
Solid yellow	Solid yellow	Power applied to the system.
Solid yellow	Off	Power on self test (POST); 9 seconds.
Solid yellow	Solid yellow	System initialization; 14 seconds.
Solid green	Solid yellow	Kernet initialization; 8 seconds.
Solid green	Flashing green	Services initialization; 1 minute.
Solid green	Solid green	System running; normal operation.
Solid green	Solid red	Services initialization failure
<b>Safe mode start-up sequence</b>		
Solid red	Solid green	System running with manufacturing settings enabled
Solid red	Solid red	System running in software reset mode
Solid red	Flashing yellow	System running in configuration reset mode
<b>Shutdown sequence or failure</b>		
Solid green	Flashing yellow	Shutdown in progress

**Table 12 System status LEDs states and descriptions**

<b>Power</b>	<b>Status</b>	<b>Description</b>
Off	Solid yellow	Shutdown completed
Solid red	Flashing yellow	Overheating detected; thermal shutdown completed
Solid red	Solid red	Power spike or rail power fluctuation detected
Flashing red	Solid red	Rail power fluctuation; power monitor shutdown completed
Solid yellow	Solid red	Power spike shutdown completed
Off	Off	No power; system is shut down
<b>Start-up profile sequence</b>		
Flashing yellow	Flashing yellow	Start-up profile executing
Flashing green	Flashing green	Start-up profile completed (USB device can be removed)
Solid green	Solid green	Start-up profile successfully applied
Solid green	Solid red	Start-up profile failure

---

## List of alarms

---

This section contains a list of alarms generated by the BCM450 system.

The table below includes information about the default handling of each alarm with respect to the Alarms table, LEDs, and SNMP traps.

You can customize whether each alarm appears in the Alarms table or is sent as an SNMP trap in accordance with your business requirements.

Alarm ID	Severity	Component Name	Problem Description	Problem Resolution	Alarm	SNMP	LED
18	minor	Core Telephony	Core Telephony - Unable to process calls.	Reboot system and contact your local support group.	Yes	No	No
31	critical	Core Telephony	Core Telephony - Media Bay Module firmware download failed.	Power down the system and check the DTM hardware and the expansion chassis connections. If problem persists replace the DTM or expansion chassis hardware.	Yes	Yes	Yes

## 64 List of alarms

---

32	critical	Core Telephony	Core Telephony - BRI module is primary clock instead of DTM module.	Configure the DTM module as primary clock in your system. BRI clock specifications are not acceptable for DTM connections to the public network.	Yes	Yes	Yes
33	critical	Core Telephony	Core Telephony - Cold restart has occurred causing loss of telephony data.	Check configuration change logs to see if this was user initiated. If not contact your local support group.	Yes	Yes	Yes
34	warning	Core Telephony	Core Telephony - Media Bay Module firmware download started.	No Action Required.	Yes	No	No



---

35	critical	Core Telephony	Core Telephony - Media Bay Module firmware download failure.	Power down the system and check the expansion chassis connections. Check for corresponding alarm 31 or 79 to determine which module is having issues. If problem persists replace corresponding hardware.	Yes	Yes	Yes
36	critical	Core Telephony	Core Telephony - Media Bay Module firmware download failure.	Power down the system and check the expansion chassis connections. Check for corresponding alarm 31 or 79 to determine which module is having issues. If problem persists replace corresponding hardware.	Yes	Yes	Yes

66 List of alarms

37	critical	Core Telephony	Core Telephony - Failure to download market profile/protocol data from the Persistent Data Repository.	Restart system and contact your local support group.	Yes	Yes	Yes
39	critical	Core Telephony	Core Telephony - Persistent Data Repository corruption in the market profile area.	Perform a restore with a known good backup. If problem persists contact your local support group.	Yes	Yes	Yes
40	critical	Core Telephony	Core Telephony - "Unavailable Seconds Error" long term alarm threshold has been exceeded on the DTM.	Check your cabling from any DTM modules to the external network and run loopback tests on the circuit to check for network issues. Get your network provider to check the circuit during problem conditions.	Yes	Yes	Yes

41	critical	Core Telephony	Core Telephony - "Loss of Signal" long term alarm threshold has been exceeded on the DTM.	Check your cabling from any DTM modules to the external network and run loopback tests on the circuit to check for network issues. Get your network provider to check the circuit during problem conditions.	Yes	Yes	Yes
42	critical	Core Telephony	Core Telephony - "Loss of Frame" long term alarm threshold has been exceeded on the DTM.	Check your cabling from any DTM modules to the external network and run loopback tests on the circuit to check for network issues. Get your network provider to check the circuit during problem conditions.	Yes	Yes	Yes

68 List of alarms

43	critical	Core Telephony	Core Telephony - "Alarm Indication Signal" long term alarm threshold has been exceeded on the DTM.	Check your cabling from any DTM modules to the external network and run loopback tests on the circuit to check for network issues. Get your network provider to check the circuit during problem conditions.	Yes	Yes	Yes
44	critical	Core Telephony	Core Telephony - "Remote Alarm Indication" long term alarm threshold has been exceeded on the DTM.	Check your cabling from any DTM modules to the external network and run loopback tests on the circuit to check for network issues. Get your network provider to check the circuit during problem conditions.	Yes	Yes	Yes

45	critical	Core Telephony	Core Telephony - "Loss of Signal" long term alarm threshold has been exceeded on the DTM.	Check your cabling from any DTM modules to the external network and run loopback tests on the circuit to check for network issues. Get your network provider to check the circuit during problem conditions.	Yes	Yes	Yes
46	critical	Core Telephony	Core Telephony - "Alarm Indication Signal" long term alarm threshold has been exceeded on the DTM.	Check your cabling from any DTM modules to the external network and run loopback tests on the circuit to check for network issues. Get your network provider to check the circuit during problem conditions.	Yes	Yes	Yes

## 70 List of alarms

---

47	critical	Core Telephony	Core Telephony - "Remote Alarm Indication" long term alarm threshold has been exceeded on the DTM.	Check your cabling from any DTM modules to the external network and run loopback tests on the circuit to check for network issues. Get your network provider to check the circuit during problem conditions.	Yes	Yes	Yes
50	critical	Core Telephony	Core Telephony - A digital station module has been disconnected.	Power down the system and check all connections to the expansion chassis containing the digital station module. If the problem persists, replace the module.	Yes	Yes	Yes

51	critical	Core Telephony	Core Telephony - A trunk media bay module has been disconnected.	Power down the system and check all connections to the expansion chassis containing the digital or analog trunk module. If the problem persists, replace the module.	Yes	Yes	Yes
52	critical	Core Telephony	Core Telephony - A trunk media bay module has been disconnected.	Power down the system and check all connections to the expansion chassis containing the digital or analog trunk module. If the problem persists, replace the module.	Yes	Yes	Yes
54	warning	Core Telephony	Core Telephony - Media Bay Module firmware download started.	No Action Required.	Yes	No	No
55	warning	Core Telephony	Core Telephony - Media Bay Module firmware download complete.	No Action Required.	Yes	No	No

## 72 List of alarms

---

61	critical	Core Telephony	Core Telephony - A trunk media bay module is programmed as the wrong module type.	Check that the correct module type is programmed for the expansion chassis.	Yes	Yes	Yes
62	critical	Core Telephony	Core Telephony - Persistent Data Repository corruption in the auto answer area.	Perform a restore with a known good backup. If problem persists contact your local support group.	Yes	Yes	Yes
63	critical	Core Telephony	Core Telephony - No DTMF receivers available.	If this happens more than once in a 5 minute span check that any auto answer or DISA configured trunks are operating properly. If they are not operating properly reboot the system and contact your local support group.	Yes	Yes	Yes



67	critical	Core Telephony	Core Telephony - Invalid trunk media bay module connected to an expansion chassis.	Power down the system and check all connections to the expansion chassis containing the digital or analog trunk module. Check that the hardware being used is supported in the market your have selected in Core Telephony. If the problem persists, replace the module.	Yes	Yes	Yes
68	critical	Core Telephony	Core Telephony - Unsupported set/peripheral connected.	Disconnect the set/peripheral from the port and reconnect it to a valid port. If the problem persists replace the set/peripheral.	Yes	Yes	Yes
69	critical	Core Telephony	Core Telephony - General software error.	Reboot system and contact your local support group.	Yes	Yes	Yes

## 74 List of alarms

---

71	warning	Core Telephony	Core Telephony - Emergency transfer relay activated indicating a power issue or Core Telephony down condition.	No Action Required.	Yes	No	No
72	critical	Core Telephony	Core Telephony - TEI request on ISDN device on system.	Disconnect all station side ISDN devices. If problem persists contact your local support group.	Yes	Yes	Yes
75	critical	Core Telephony	Core Telephony - Digital trunking clock in free run.	Check your cabling from any DTM modules to the external network. Get your network provider to check the circuit.	Yes	Yes	Yes
77	critical	Core Telephony	Core Telephony - Persistent Data Repository corruption.	Perform a restore with a known good backup. If problem persists contact your local support group.	Yes	Yes	Yes

79	critical	Core Telephony	Core Telephony - ASM firmware download error.	Power down the system and check the ASM hardware and the expansion chassis connections. If problem persists replace the ASM or expansion chassis hardware.	Yes	Yes	Yes
194	critical	Core Telephony	Core Telephony - Low Level Operating error.	Restart system and contact your local support group.	Yes	Yes	Yes
224	critical	Core Telephony	Core Telephony - Error after restore of data.	Attempt another restore with a known good backup. If problem persists contact your local support group.	Yes	Yes	Yes

76 List of alarms

247	critical	Core Telephony	Core Telephony - Digital station loop error.	Verify that all types of attached sets/peripherals initialize and function. If something is not working reset it. If the problem persists contact your local support group.	Yes	Yes	Yes
260	minor	Core Telephony	Core Telephony - Line presence test failure on system startup due to no battery feed on a trunk line.	Verify all trunks lines are connected to the system and in working condition. If not disable/enable the trunk interfaces. If problems persists contact your local support group.	Yes	No	No
262	minor	Core Telephony	Core Telephony - No dialtone on trunk line during seizure.	Check the trunk interfaces to see if dialtone is present. If no dialtone is present contact your network provider.	Yes	No	No

---

263	minor	Core Telephony	Core Telephony - Invalid disconnect sequence error on an analog trunk line.	Check the analog trunk interfaces to ensure all lines are operating correctly. If a trunk is showing busy with no active calls disable the trunk interface and re-enable it. If problems persist contact your local support group.	Yes	No	No
265	minor	Core Telephony	Core Telephony - Outgoing trunk could not be seized. Handshake between the system and network failed.	Check the trunk interfaces to ensure all lines are operating correctly. If a trunk is not able to be used contact your network provider.	Yes	No	No

## 78 List of alarms

---

270	minor	Core Telephony	Core Telephony - Set initialization error from an invalid message from the set.	If the event occurs more than once in a 5 minute span then disconnect the set in question. If problem stops replace set and check cable between set and system.	Yes	No	No
271	minor	Core Telephony	Core Telephony - A set is trying to initialize that has incompatible firmware on the system.	Verify that all types of attached sets/peripherals initialize and function. If something is not working reset it. If the problem persists contact your local support group.	Yes	No	No

323	minor	Core Telephony	Core Telephony - "Degraded Minute" short term alarm threshold has been exceeded on the DTM. The module is in a no-new-calls state.	Check your cabling from any DTM modules to the external network and run loopback tests on the circuit to check for network issues. If long term alarms occur get your network provider to check the circuit during problem conditions.	Yes	No	No
324	minor	Core Telephony	Core Telephony - "Severely Errored Second" short term alarm threshold has been exceeded on the DTM. The module is in a no-new-calls state.	Check your cabling from any DTM modules to the external network and run loopback tests on the circuit to check for network issues. If long term alarms occur get your network provider to check the circuit during problem conditions.	Yes	No	No

80 List of alarms

325	minor	Core Telephony	Core Telephony - "Errored Second" short term alarm threshold has been exceeded on the DTM. The module is in a no-new-calls state.	Check your cabling from any DTM modules to the external network and run loopback tests on the circuit to check for network issues. If long term alarms occur get your network provider to check the circuit during problem conditions.	Yes	No	No
326	minor	Core Telephony	Core Telephony - "Slip Underflow" short term alarm threshold has been exceeded on the DTM. The module is in a no-new-calls state.	Check your cabling from any DTM modules to the external network and run loopback tests on the circuit to check for network issues. If long term alarms occur get your network provider to check the circuit during problem conditions.	Yes	No	No



327	minor	Core Telephony	Core Telephony - "Slip Overflow" short term alarm threshold has been exceeded on the DTM. The module is in a no-new-calls state.	Check your cabling from any DTM modules to the external network and run loopback tests on the circuit to check for network issues. If long term alarms occur get your network provider to check the circuit during problem conditions.	Yes	No	No
328	minor	Core Telephony	Core Telephony - "Line Code Violation" short term alarm threshold has been exceeded on the DTM. The module is in a no-new-calls state.	Check your cabling from any DTM modules to the external network and run loopback tests on the circuit to check for network issues. If long term alarms occur get your network provider to check the circuit during problem conditions.	Yes	No	No

82 List of alarms

329	minor	Core Telephony	Core Telephony - "Loss of Signal" short term alarm threshold has been exceeded on the DTM. The module is in a no-new-calls state.	Check your cabling from any DTM modules to the external network and run loopback tests on the circuit to check for network issues. If long term alarms occur get your network provider to check the circuit during problem conditions.	Yes	No	No
330	minor	Core Telephony	Core Telephony - "Loss of Frame" short term alarm threshold has been exceeded on the DTM. The module is in a no-new-calls state.	Check your cabling from any DTM modules to the external network and run loopback tests on the circuit to check for network issues. If long term alarms occur get your network provider to check the circuit during problem conditions.	Yes	No	No

331	minor	Core Telephony	Core Telephony - "Alarm Indication" short term alarm threshold has been exceeded on the DTM. The module is in a no-new-calls state.	Check your cabling from any DTM modules to the external network and run loopback tests on the circuit to check for network issues. If long term alarms occur get your network provider to check the circuit during problem conditions.	Yes	No	No
332	minor	Core Telephony	Core Telephony - "Remote Alarm Indication" short term alarm threshold has been exceeded on the DTM. The module is in a no-new-calls state.	Check your cabling from any DTM modules to the external network and run loopback tests on the circuit to check for network issues. If long term alarms occur get your network provider to check the circuit during problem conditions.	Yes	No	No

84 List of alarms

---

333	minor	Core Telephony	Core Telephony - "Loss of Frame" short term alarm threshold has been exceeded on the DTM. The module is in a no-new-calls state.	Check your cabling from any DTM modules to the external network and run loopback tests on the circuit to check for network issues. If long term alarms occur get your network provider to check the circuit during problem conditions.	Yes	No	No
334	minor	Core Telephony	Core Telephony - "Alarm Indication" short term alarm threshold has been exceeded on the DTM. The module is in a no-new-calls state.	Check your cabling from any DTM modules to the external network and run loopback tests on the circuit to check for network issues. If long term alarms occur get your network provider to check the circuit during problem conditions.	Yes	No	No

335	minor	Core Telephony	Core Telephony - "Remote Alarm Indication" short term alarm threshold has been exceeded on the DTM. The module is in a no-new-calls state.	Check your cabling from any DTM modules to the external network and run loopback tests on the circuit to check for network issues. If long term alarms occur get your network provider to check the circuit during problem conditions.	Yes	No	No
336	information	Core Telephony	Core Telephony - The Digital Trunk T1/E1/PRI has recovered.	No Action Required.	Yes	No	No
367	minor	Core Telephony	Core Telephony - Digital Trunk Media bay module reset.	Determine whether this alarm occurred due to the system rebooting. If the system was not rebooting when the alarm occurred, then contact your local support group.	Yes	No	No

86 List of alarms

372	warning	Core Telephony	Core Telephony - Clocking on the Digital Trunk Media bay module has changed sources.	No Action Required.	Yes	No	No
401	minor	Core Telephony	Core Telephony - Digital station loop initialization error.	Verify that all types of attached sets/peripherals initialize and function. If something is not working reset it. If the problem persists contact your local support group.	Yes	No	No
608	minor	Core Telephony	Core Telephony - Unsupported set/peripheral connected.	Verify that all types of attached sets/peripherals initialize and function. Remove any unsupported set types.	Yes	No	No
639	minor	Core Telephony	Core Telephony - CAP/KIM error while retrieving key information.	Check the system for CAP/KIM modules and reset them. If the problem persists contact your local support group.	Yes	No	No

799	minor	Core Telephony	Core Telephony - ISDN call processing error.	No Action Required.	Yes	No	No
894	minor	Core Telephony	Core Telephony - DASS2/DPNSS error on a DTM module.	Check that the DASS2/DPNSS circuit is online. If it is not disable/enable the expansion chassis and try to get the circuit back online. If problem persists contact your local support group.	Yes	No	No
901	critical	Core Telephony	Core Telephony - Persistent Data Repository corruption.	Restore a known good backup into the system to get it back online and contact your local support group.	Yes	Yes	Yes
949	minor	Core Telephony	Core Telephony - BRI protocol call control error.	Get a protocol trace of the BRI loop using BCM monitor and contact your local support group.	Yes	No	No
950	information	Set Template Programming	A template has failed to be applied to a set.	No Action Required.	Yes	No	No

88 List of alarms

999	warning	Core Telephony	Core Telephony - Unknown alarm.	Contact your local support group.	Yes	No	No
1001	major	Operating System	Operating System - Major operating system error (Kernel Oops).	Contact your local support group.	Yes	Yes	Yes
1002	critical	Operating System	Operating System - Critical operating system error (Kernel panic).	Contact your local support group.	Yes	Yes	Yes
1003	major	Operating System	A USB device could not be mounted. Two USB storage devices are attached to the system. This is an unsupported configuration.	Please remove one of the devices and retry the operation.	Yes	Yes	Yes
2100	information	Software Updates	Software Update - Software update applied successfully.	No Action Required.	Yes	No	No
2101	information	Software Updates	Software Update - Software upgrade applied successfully.	No Action Required.	Yes	No	No
2102	information	Software Updates	Software Update - Software update started.	No Action Required.	Yes	No	No
2103	information	Software Updates	Software Update - Software upgrade started.	No Action Required.	Yes	No	No
2104	information	Software Updates	Software Update - Software update scheduled.	No Action Required.	Yes	No	No
2105	information	Software Updates	Software Update - Scheduled software update completed.	No Action Required.	Yes	No	No
2106	information	Software Updates	Software Update - Software update removed.	No Action Required.	Yes	No	No
2300	critical	Software Updates	Software Update - Software update failed to apply.	Contact your local support group.	Yes	Yes	Yes



2301	major	Software Updates	Software Update - Software update failed to transfer files.	Retry software update and if problem persists contact your local support group.	Yes	Yes	Yes
2302	critical	Software Updates	Software Update - Software upgrade failed to apply.	Contact your local support group.	Yes	Yes	Yes
2303	major	Software Updates	Software Update - Failed to remove software update.	Retry removal of software update and if problem persists contact your local support group.	Yes	Yes	Yes
2304	major	Software Updates	Software Update - Software update invalid signature or corrupt file. Retry file transfer.	Retry software update and if problem persists contact your local support group.	Yes	Yes	Yes
5001	critical	Persistent Data Repository	Persistent Data Repository - Could not start Persistent Data Repository. No resources available. This will cause many components to fail to start with the proper configuration.	Reboot system and contact your local support group.	Yes	Yes	Yes

## 90 List of alarms

5002	critical	Persistent Data Repository	Persistent Data Repository - Could not open Persistent Data Repository. Reverting to last saved file. Will mean configuration will not be current on the system.	Restore a known good backup into the system . If the problem persists contact your local support group.	Yes	Yes	Yes
5003	critical	Persistent Data Repository	Persistent Data Repository - Could not open Persistent Data Repository. Reverting to default file. Will mean configuration will be default on the system.	Restore a known good backup into the system . If the problem persists contact your local support group.	Yes	Yes	Yes
6000	minor	Date and Time	Date and Time - Time has been updated by CoreTel.	No Action Required.	Yes	No	No
6004	critical	Date and Time	Date and Time - Time service initialization failed.	Contact your local support group.	Yes	Yes	Yes
6007	minor	Date and Time	Date and Time - Time adjustment detected which is larger than provisioned.	Confirm the date/time is correct on the system.	Yes	No	No
6008	minor	Date and Time	Date and Time - NTP client unable to contact server.	Confirm the NTP server is available on the network.	Yes	No	No

6010	critical	Date and Time	Date and Time - Real time clock on system not working properly.	Don't reboot the system and contact your local support group.	Yes	Yes	Yes
8001	critical	Modem Call Control	Modem Call Control - MCC stopped unexpectedly.	Reboot system and contact your local support group.	Yes	Yes	Yes
8002	critical	Modem Call Control	Modem Call Control - MCC Failed to Register with Voice CTI.	Reboot system and contact your local support group.	Yes	Yes	Yes
8003	Warning	Modem Call Control	Modem Call Control - MCC cannot load modem to DSP error.	Contact your local support group.	Yes	No	No
8004	critical	Modem Call Control	Modem Call Control - MCC modem emulator failed to start.	Reboot system and contact your local support group.	Yes	Yes	Yes
8005	critical	Modem Call Control	Modem Call Control - MCC failed to get a modem DN.	Reboot system and contact your local support group.	Yes	Yes	Yes
8008	critical	Modem Call Control	Modem Call Control - MCC state machine error.	Reboot system and contact your local support group.	Yes	Yes	Yes
8009	critical	Modem Call Control	Modem Call Control - MCC state machine error.	Reboot system and contact your local support group.	Yes	Yes	Yes

92 List of alarms

8010	critical	Modem Call Control	Modem Call Control - MCC state machine error.	Reboot system and contact your local support group.	Yes	Yes	Yes
8011	critical	Modem Call Control	Modem Call Control - MCC state machine error.	Reboot system and contact your local support group.	Yes	Yes	Yes
8012	Warning	Modem Call Control	Modem Call Control - MCC Failed to Transfer the call. CTI Return Code = %ld.	Contact your local support group.	Yes	No	No
8013	Warning	Modem Call Control	Modem Call Control - MCC Cannot Monitor Incoming Line. CTI Return Code = %ld.	Reboot system and contact your local support group.	Yes	No	No
8014	Warning	Modem Call Control	Modem Call Control - MCC Can only Transfer to Modem DN Manually. CTI Return Code = %ld.	Contact your local support group.	Yes	No	No
8015	Warning	Modem Call Control	Modem Call Control - MCC Cannot Stop to Monitor the Line Number. CTI Return Code = %ld.	Contact your local support group.	Yes	No	No

8016	Warning	Modem Call Control	Modem Call Control - MCC Cannot Unload the Modem DSP Task. CTI Return Code = %ld.	Contact your local support group.	Yes	No	No
8017	Warning	Modem Call Control	Modem Call Control - MCC Failed to Answer Incoming Call. CTI Return Code = %ld.	Contact your local support group.	Yes	No	No
8018	information	Modem Call Control	Modem Call Control - MCC Incoming Call on Busy Modem [%s].	No Action Required.	Yes	No	No
8019	information	Modem Call Control	Modem Call Control - MCC Attempt to Connect to a Disabled Modem [%s].	No Action Required.	Yes	No	No
8020	Warning	Modem Call Control	Modem Call Control - MCC Failed to Register for CLID/ANI Service. CTI Return Code = %ld.	Contact your local support group.	Yes	No	No
8021	information	Modem Call Control	Modem Call Control - MCC Modem Connected [%s].	No Action Required.	Yes	No	No

94 List of alarms

8022	information	Modem Call Control	Modem Call Control - MCC Modem is Disconnected.	No Action Required.	Yes	No	No
8023	information	Modem Call Control	Modem Call Control - MCC Modem Enabled.	No Action Required.	Yes	No	No
8024	information	Modem Call Control	Modem Call Control - MCC Modem Disabled.	No Action Required.	Yes	No	No
8025	Warning	Modem Call Control	Modem Call Control - MCC Failed to Get Switch Information. CTI Return Code = %ld.	Contact your local support group.	Yes	No	No
8029	Warning	Modem Call Control	Modem Call Control - MCC Failed to Answer Modem Call. CTI Return Code = %ld.	Contact your local support group.	Yes	No	No
8030	Warning	Modem Call Control	Modem Call Control - MCC Failed to Acknowledge Modem Request. CTI Return Code = %ld.	Contact your local support group.	Yes	No	No
8031	Warning	Modem Call Control	Modem Call Control - MCC Failed to Originate a Call. CTI Return Code = %ld.	Contact your local support group.	Yes	No	No

8032	Warning	Modem Call Control	Modem Call Control - MCC Failed to Disconnect a Call. CTI Return Code = %ld.	Contact your local support group.	Yes	No	No
8033	Warning	Modem Call Control	Modem Call Control - MCC Received Unknown Request from Modem. Request = %ld.	Contact your local support group.	Yes	No	No
8035	information	Modem Call Control	Modem Call Control - MCC Modem Auto Disabled.	No Action Required.	Yes	No	No
8038	information	Modem Call Control	Modem Call Control - MCC Modem Call Put on Hold. Disconnecting...	No Action Required.	Yes	No	No
8040	Warning	Modem Call Control	Modem Call Control - MCC Failed to Open Prompts Library. NNU Return Code = %ld.	Contact your local support group.	Yes	No	No
8041	information	Modem Call Control	Modem Call Control - MCC Modem DN changed in admin.	No Action Required.	Yes	No	No

96 List of alarms

8042	Warning	Modem Call Control	Modem Call Control - MCC Failed to Open the Communication Path to RAS. Disabling the Modem.	Contact your local support group.	Yes	No	No
10001	critical	Service Manager	Service Manager - Core Telephony has stopped unexpectedly. Service Manager is attempting to restart the service.	Check for corresponding alarm 10101 or 10301. If service doesn't restart then reboot system and contact your local support group.	Yes	Yes	Yes
10002	critical	Service Manager	Service Manager - CallPilot has stopped unexpectedly. Service Manager is attempting to restart the service.	Check for corresponding alarm 10102 or 10302. If service doesn't restart then reboot system and contact your local support group.	Yes	Yes	Yes



10003	critical	Service Manager	Service Manager - IP Terminal Service (UTPS) has stopped unexpectedly. This will affect service on all IP terminals on the system. Service Manager is attempting to restart the service.	Check for corresponding alarm 10103 or 10303. If service doesn't restart then reboot system and contact your local support group.	Yes	Yes	Yes
10005	critical	Service Manager	Service Manager - Voice over IP Gateway (feps) has stopped unexpectedly. Service Manager is attempting to restart the service.	Check for corresponding alarm 10105 or 10305. If service doesn't restart then reboot system and contact your local support group.	Yes	Yes	Yes
10006	critical	Service Manager	Service Manager - Quality of Service Monitor (qmond) has stopped unexpectedly. Service Manager is attempting to restart the service.	Check for corresponding alarm 10106 or 10306. If service doesn't restart then reboot system and contact your local support group.	Yes	Yes	Yes

## 98 List of alarms

---

10007	critical	Service Manager	Service Manager - Call Detail Recording Service (CDRService) has stopped unexpectedly. Service Manager is attempting to restart the service.	Check for corresponding alarm 10107 or 10307. If service doesn't restart then reboot system and contact your local support group.	Yes	Yes	Yes
10008	critical	Service Manager	Service Manager - Voice Application Interface Service (ctiserver) has stopped unexpectedly. This will affect CallPilot, System Set Based Admin and the modem. Service Manager is attempting to restart the service.	Check for corresponding alarm 10108 or 10308. If service doesn't restart then reboot system and contact your local support group.	Yes	Yes	Yes

10008	critical	Service Manager	Service Manager - Voice Application Interface Service (ctiserver) has stopped unexpectedly. This will affect CallPilot, System Set Based Admin and IVR. Service Manager is attempting to restart the service.	Check for corresponding alarm 10108 or 10308. If service doesn't restart then reboot system and contact your local support group.	Yes	Yes	Yes
10009	critical	Service Manager	Service Manager - Modem Call Control (modemcc) has stopped unexpectedly. This will affect Dial-In and Dial-Out using the integrated modem. Service Manager is attempting to restart the service.	Check for corresponding alarm 10109 or 10309. If service doesn't restart then reboot system and contact your local support group.	Yes	Yes	Yes

100 List of alarms

---

10010	critical	Service Manager	Service Manager - System Set Based Admin Feature9*8 (ssba) has stopped unexpectedly. Service Manager is attempting to restart the service.	Check for corresponding alarm 10110 or 10310. If service doesn't restart then reboot system and contact your local support group.	Yes	Yes	Yes
10011	critical	Service Manager	Service Manager - Computer Telephony Service (Cte) has stopped unexpectedly. This will affect LAN CTE and the Line Monitor in BCM Monitor. Service Manager is attempting to restart the service.	Check for corresponding alarm 10111 or 10311. If service doesn't restart then reboot system and contact your local support group.	Yes	Yes	Yes

10012	critical	Service Manager	Service Manager - Line Monitor Service (lms) has stopped unexpectedly. This will affect the Line Service Manager - Monitor in BCM Monitor. Service Manager is attempting to restart the service.	Check for corresponding alarm 10112 or 10312. If service doesn't restart then reboot system and contact your local support group.	Yes	Yes	Yes
10013	critical	Service Manager	Service Manager - Media Services Manager (Msm) has stopped unexpectedly. This will affect all telephony operations on the system. Service Manager is attempting to restart the service.	Check for corresponding alarm 10113 or 10313. If service doesn't restart then reboot system and contact your local support group.	Yes	Yes	Yes

102 List of alarms

10014	critical	Service Manager	Service Manager - Media Path Server (mps) has stopped unexpectedly. This will affect all IP Telephony. Service Manager is attempting to restart the service.	Check for corresponding alarm 10114 or 10314. If service doesn't restart then reboot system and contact your local support group.	Yes	Yes	Yes
10015	critical	Service Manager	Service Manager - Media Gateway Server (mgs) has stopped unexpectedly. This will affect all IP Telephony. Service Manager is attempting to restart the service.	Check for corresponding alarm 10115 or 10315. If service doesn't restart then reboot system and contact your local support group.	Yes	Yes	Yes
10016	critical	Service Manager	Service Manager - Persistent Data Repository (Pdrd) has stopped unexpectedly. This will affect any management done to running services or startup of non-running services. Service Manager is attempting to restart the service.	Check for corresponding alarm 10116 or 10316. If service doesn't restart then reboot system and contact your local support group.	Yes	Yes	Yes

---

10017	critical	Service Manager	Service Manager - Keycode Service (cfsserver) has stopped unexpectedly. This will affect the ability to enter any new keycodes. Service Manager is attempting to restart the service.	Check for corresponding alarm 10117 or 10317. If service doesn't restart then reboot system and contact your local support group.	Yes	Yes	Yes
10018	critical	Service Manager	Service Manager - Time Service (tmwservice) has stopped unexpectedly. This will affect the synchronization of time in the system. Service Manager is attempting to restart the service.	Check for corresponding alarm 10118 or 10318. If service doesn't restart then reboot system and contact your local support group.	Yes	Yes	Yes

104 List of alarms

---

10019	critical	Service Manager	Service Manager - Platform Status Monitor (psm) has stopped unexpectedly. This will affect the monitoring of system hardware and drivers. Service Manager is attempting to restart the service.	Check for corresponding alarm 10119 or 10319. If service doesn't restart then reboot system and contact your local support group.	Yes	Yes	Yes
10020	critical	Service Manager	Service Manager - Web Server (httpd) has stopped unexpectedly. This will affect the onbox web pages, downloads and documentation. Service Manager is attempting to restart the service.	Check for corresponding alarm 10120 or 10320. If service doesn't restart then reboot system and contact your local support group.	Yes	Yes	Yes



10021	critical	Service Manager	Service Manager - On Box Management Framework (owcimomd) has stopped unexpectedly. Element Manager will be unable to connect with the system. Service Manager is attempting to restart the service.	Check for corresponding alarm 10121 or 10321. If service doesn't restart then reboot system and contact your local support group.	Yes	Yes	Yes
10024	critical	Service Manager	Service Manager - IP Terminal Service (EchoServer) has stopped unexpectedly. This will affect IP terminals from operating properly. Service Manager is attempting to restart the service.	Check for corresponding alarm 10124 or 10324. If service doesn't restart then reboot system and contact your local support group.	Yes	Yes	Yes

106 List of alarms

10025	critical	Service Manager	Service Manager - IP Terminal Firmware upload Service (UftpServer) has stopped unexpectedly. This will affect the ability to download new firmware to IP terminals. Service Manager is attempting to restart the service.	Check for corresponding alarm 10125 or 10325. If service doesn't restart then reboot system and contact your local support group.	Yes	Yes	Yes
10029	critical	Service Manager	Service Manager - Doorphone service (BCM_Doorphone) has stopped unexpectedly. This will affect the ability to use a doorphone on the system. Service Manager is attempting to restart the service.	Check for corresponding alarm 10129 or 10329. If service doesn't restart then reboot system and contact your local support group.	Yes	Yes	Yes

10032	minor	Service Manager	Service Manager - IP Music Service (BcmAmp) has stopped unexpectedly. This will affect the ability to use IP music. Service Manager is attempting to restart the service.	Check for corresponding alarm 10132 or 10332. If service doesn't restart then reboot system and contact your local support group.	Yes	Yes	Yes
10033	minor	Service Manager	Service Manager - IP Music Service (ToneSrvr) has stopped unexpectedly. This will affect the ability to use IP music. Service Manager is attempting to restart the service.	Check for corresponding alarm 10133 or 10333. This can be caused by changing music sources. If service doesn't restart then reboot system and contact your local support group..	Yes	No	No
10101	critical	Service Manager	Service Manager - Core Telephony has stopped unexpectedly and could not be restarted by service manager.	Reboot system and contact your local support group.	Yes	Yes	Yes

108 List of alarms

---

10102	critical	Service Manager	Service Manager - CallPilot has stopped unexpectedly and could not be restarted by service manager.	Reboot system and contact your local support group.	Yes	Yes	Yes
10103	critical	Service Manager	Service Manager - IP Terminal Service (UTPS) has stopped unexpectedly and could not be restarted by service manager. This will affect service on all IP terminals on the system.	Reboot system and contact your local support group.	Yes	Yes	Yes
10105	critical	Service Manager	Service Manager - Voice over IP Gateway (feps) has stopped unexpectedly and could not be restarted by service manager.	Reboot system and contact your local support group.	Yes	Yes	Yes

10106	critical	Service Manager	Service Manager - Quality of Service Monitor (qmond) has stopped unexpectedly and could not be restarted by service manager.	Reboot system and contact your local support group.	Yes	Yes	Yes
10107	critical	Service Manager	Service Manager - Call Detail Recording Service (CDRService) has stopped unexpectedly and could not be restarted by service manager.	Reboot system and contact your local support group.	Yes	Yes	Yes
10108	critical	Service Manager	Service Manager - Voice Application Interface Service (ctiserver) has stopped unexpectedly and could not be restarted by service manager. This will affect CallPilot, System Set Based Admin and the modem.	Reboot system and contact your local support group.	Yes	Yes	Yes

110 List of alarms

---

10109	critical	Service Manager	Service Manager - Modem Call Control (modemcc) has stopped unexpectedly and could not be restarted by service manager. This will affect Dial-In and Dial-Out using the integrated modem.	Reboot system and contact your local support group.	Yes	Yes	Yes
10110	critical	Service Manager	Service Manager - System Set Based Admin Feature9*8 (ssba) has stopped unexpectedly and could not be restarted by service manager.	Reboot system and contact your local support group.	Yes	Yes	Yes

10111	critical	Service Manager	Service Manager - Computer Telephony Service (Cte) has stopped unexpectedly and could not be restarted by service manager. This will affect LAN CTE and the Line Monitor in BCM Monitor.	Reboot system and contact your local support group.	Yes	Yes	Yes
10112	critical	Service Manager	Service Manager - Line Monitor Service (lms) has stopped unexpectedly and could not be restarted by service manager. This will affect the Line Monitor in BCM Monitor.	Reboot system and contact your local support group.	Yes	Yes	Yes

112 List of alarms

10113	critical	Service Manager	Service Manager - Media Services Manager (Msm) has stopped unexpectedly and could not be restarted by service manager. This will affect all telephony operations on the system.	Reboot system and contact your local support group.	Yes	Yes	Yes
10114	critical	Service Manager	Service Manager - Media Path Server (mps) has stopped unexpectedly and could not be restarted by service manager. This will affect all IP Telephony.	Reboot system and contact your local support group.	Yes	Yes	Yes
10115	critical	Service Manager	Service Manager - Media Gateway Server (mgs) has stopped unexpectedly and could not be restarted by service manager. This will affect all IP Telephony.	Reboot system and contact your local support group.	Yes	Yes	Yes



---

10116	critical	Service Manager	Service Manager - Persistent Data Repository (Pdrd) has stopped unexpectedly and could not be restarted by service manager. This will affect any management done to running services or startup of non-running services.	Reboot system and contact your local support group.	Yes	Yes	Yes
10117	critical	Service Manager	Service Manager - Keycode Service (cfsserver) has stopped unexpectedly and could not be restarted by service manager. This will affect the ability to enter any new keycodes.	Reboot system and contact your local support group.	Yes	Yes	Yes

114 List of alarms

---

10118	critical	Service Manager	Service Manager - Time Service (tmwservice) has stopped unexpectedly and could not be restarted by service manager. This will affect the synchronization of time in the system.	Reboot system and contact your local support group.	Yes	Yes	Yes
10119	critical	Service Manager	Service Manager - Platform Status Monitor (psm) has stopped unexpectedly and could not be restarted by service manager. This will affect the monitoring of system hardware and drivers.	Reboot system and contact your local support group.	Yes	Yes	Yes

---

10120	critical	Service Manager	Service Manager - Web Server (httpd) has stopped unexpectedly and could not be restarted by service manager. This will affect the onbox web pages, downloads and documentation.	Reboot system and contact your local support group.	Yes	Yes	Yes
10121	critical	Service Manager	Service Manager - On Box Management Framework (owcimomd) has stopped unexpectedly and could not be restarted by service manager. Element Manager will be unable to connect with the system.	Reboot system and contact your local support group.	Yes	Yes	Yes

116 List of alarms

---

10122	critical	Service Manager	Service Manager - Service Manager (monit) has stopped unexpectedly.	Check for corresponding alarm 10322 to indicate a restart. If 10322 doesn't happen then reboot system and contact your local support group.	Yes	Yes	Yes
10124	critical	Service Manager	Service Manager - IP Terminal Service (EchoServer) has stopped unexpectedly and could not be restarted by service manager. This will affect IP terminals from operating properly.	Reboot system and contact your local support group.	Yes	Yes	Yes

10125	critical	Service Manager	Service Manager - IP Terminal Firmware upload Service (UftpServer) has stopped unexpectedly and could not be restarted by service manager. This will affect the ability to download new firmware to IP terminals.	Reboot system and contact your local support group.	Yes	Yes	Yes
10129	critical	Service Manager	Service Manager - Doorphone service (BCM_Doorphone) has stopped unexpectedly and could not be restarted by service manager. This will affect the ability to use a doorphone on the system.	Reboot system and contact your local support group.	Yes	Yes	Yes

118 List of alarms

---

10132	critical	Service Manager	Service Manager - IP Music Service (BcmAmp) has stopped unexpectedly and could not be restarted by service manager. This will affect the ability to use IP music.	Reboot system and contact your local support group.	Yes	Yes	Yes
10133	critical	Service Manager	Service Manager - IP Music Service (ToneSrvr) has stopped unexpectedly and could not be restarted by service manager. This will affect the ability to use IP music.	Reboot system and contact your local support group.	Yes	Yes	Yes

---

10201	Warning	Service Manager	Service Manager - Core Telephony has been stopped either due to user action or because Service Manager has stopped this service due to a dependency on another service that has been stopped.	No Action Required.	Yes	No	No
10202	Warning	Service Manager	Service Manager - CallPilot has been stopped either due to user action or because Service Manager has stopped this service due to a dependency on another service that has been stopped.	No Action Required.	Yes	No	No

120 List of alarms

---

10203	Warning	Service Manager	Service Manager - IP Terminal Service (UTPS) has been stopped either due to user action or because Service Manager has stopped this service due to a dependency on another service that has been stopped. This will affect service on all IP terminals on the system.	No Action Required.	Yes	No	No
10205	Warning	Service Manager	Service Manager - Voice over IP Gateway (feps) has been stopped either due to user action or because Service Manager has stopped this service due to a dependency on another service that has been stopped.	No Action Required.	Yes	No	No



---

10206	Warning	Service Manager	Service Manager - Quality of Service Monitor (qmond) has been stopped either due to user action or because Service Manager has stopped this service due to a dependency on another service that has been stopped.	No Action Required.	Yes	No	No
10207	Warning	Service Manager	Service Manager - Call Detail Recording Service (CDRService) has been stopped either due to user action or because Service Manager has stopped this service due to a dependency on another service that has been stopped.	No Action Required.	Yes	No	No

122 List of alarms

---

10208	Warning	Service Manager	Service Manager - Voice Application Interface Service (ctiserver) has been stopped either due to user action or because Service Manager has stopped this service due to a dependency on another service that has been stopped. This will affect Call-Pilot, System Set Based Admin and the modem.	No Action Required.	Yes	No	No
-------	---------	-----------------	---	---------------------	-----	----	----

---

10209	Warning	Service Manager	Service Manager - Modem Call Control (modemcc) has been stopped either due to user action or because Service Manager has stopped this service due to a dependency on another service that has been stopped. This will affect Dial-In and Dial-Out using the integrated modem.	No Action Required.	Yes	No	No
-------	---------	-----------------	---	---------------------	-----	----	----

124 List of alarms

---

10210	Warning	Service Manager	Service Manager - System Set Based Admin Feature9*8 (ssba) has been stopped either due to user action or because Service Manager has stopped this service due to a dependency on another service that has been stopped.	No Action Required.	Yes	No	No
-------	---------	-----------------	---	---------------------	-----	----	----

---

10211	Warning	Service Manager	Service Manager - Computer Telephony Service (Cte) has been stopped either due to user action or because Service Manager has stopped this service due to a dependency on another service that has been stopped. This will affect LAN CTE and the Line Monitor in BCM Monitor.	No Action Required.	Yes	No	No
-------	---------	-----------------	---	---------------------	-----	----	----

126 List of alarms

---

10212	Warning	Service Manager	Service Manager - Line Monitor Service (lms) has been stopped either due to user action or because Service Manager has stopped this service due to a dependency on another service that has been stopped. This will affect the Line Monitor in BCM Monitor.	No Action Required.	Yes	No	No
-------	---------	-----------------	---	---------------------	-----	----	----

---

10213	Warning	Service Manager	Service Manager - Media Services Manager (Msm) has been stopped either due to user action or because Service Manager has stopped this service due to a dependency on another service that has been stopped. This will affect all telephony operations on the system.	No Action Required.	Yes	No	No
-------	---------	-----------------	--	---------------------	-----	----	----

128 List of alarms

10214	Warning	Service Manager	Service Manager - Media Path Server (mps) has been stopped either due to user action or because Service Manager has stopped this service due to a dependency on another service that has been stopped. This will affect all IP Telephony.	No Action Required.	Yes	No	No
10215	Warning	Service Manager	Service Manager - Media Gateway Server (mgs) has been stopped either due to user action or because Service Manager has stopped this service due to a dependency on another service that has been stopped. This will affect all IP Telephony.	No Action Required.	Yes	No	No



---

10216	Warning	Service Manager	Service Manager - Persistent Data Repository (Pdrd) has been stopped either due to user action or because Service Manager has stopped this service due to a dependency on another service that has been stopped. This will affect any management done to running services.	No Action Required.	Yes	No	No
-------	---------	-----------------	--	---------------------	-----	----	----

130 List of alarms

---

10217	Warning	Service Manager	Service Manager - Keycode Service (cfserver) has been stopped either due to user action or because Service Manager has stopped this service due to a dependency on another service that has been stopped. This will affect the ability to enter any new keycodes.	No Action Required.	Yes	No	No
-------	---------	-----------------	---	---------------------	-----	----	----

---

10218	Warning	Service Manager	Service Manager - Time Service (tmwservice) has been stopped either due to user action or because Service Manager has stopped this service due to a dependency on another service that has been stopped. This will affect the synchronization of time in the system.	No Action Required.	Yes	No	No
-------	---------	-----------------	--	---------------------	-----	----	----

132 List of alarms

---

10219	Warning	Service Manager	Service Manager - Platform Status Monitor (psm) has been stopped either due to user action or because Service Manager has stopped this service due to a dependency on another service that has been stopped. This will affect the monitoring of system hardware and drivers.	No Action Required.	Yes	No	No
-------	---------	-----------------	--	---------------------	-----	----	----

---

10220	Warning	Service Manager	Service Manager - Web Server (httpd) has been stopped either due to user action or because Service Manager has stopped this service due to a dependency on another service that has been stopped. This will affect the onbox web pages, downloads and documentation.	No Action Required.	Yes	No	No
-------	---------	-----------------	--	---------------------	-----	----	----

134 List of alarms

---

10221	Warning	Service Manager	Service Manager - On Box Management Framework (owcimomd) has been stopped either due to user action or because Service Manager has stopped this service due to a dependency on another service that has been stopped. Element Manager will be unable to connect with the system.	No Action Required.	Yes	No	No
-------	---------	-----------------	--	---------------------	-----	----	----

---

10224	Warning	Service Manager	Service Manager - IP Terminal Service (EchoServer) has been stopped either due to user action or because Service Manager has stopped this service due to a dependency on another service that has been stopped. This will affect IP terminals from operating properly.	No Action Required.	Yes	No	No
-------	---------	-----------------	--	---------------------	-----	----	----

136 List of alarms

---

10225	Warning	Service Manager	Service Manager - IP Terminal Firmware upload Service (UftpServer) has been stopped either due to user action or because Service Manager has stopped this service due to a dependency on another service that has been stopped. This will affect the ability to download new firmware to IP terminals.	No Action Required.	Yes	No	No
-------	---------	-----------------	--	---------------------	-----	----	----



---

10229	Warning	Service Manager	Service Manager - Doorphone service (BCM_Doorphone) has been stopped either due to user action or because Service Manager has stopped this service due to a dependency on another service that has been stopped. This will affect the ability to use a doorphone on the system.	No Action Required.	Yes	No	No
-------	---------	-----------------	---	---------------------	-----	----	----

138 List of alarms

---

10232	Warning	Service Manager	Service Manager - IP Music Service (BcmAmp) has been stopped either due to user action or because Service Manager has stopped this service due to a dependency on another service that has been stopped. This will affect the ability to use IP music.	No Action Required.	Yes	No	No
-------	---------	-----------------	--	---------------------	-----	----	----

10233	Warning	Service Manager	Service Manager - IP Music Service (ToneSrvr) has been stopped either due to user action or because Service Manager has stopped this service due to a dependency on another service that has been stopped. This will affect the ability to use IP music.	No Action Required.	Yes	No	No
10301	Information	Service Manager	Service Manager - Core Telephony has been successfully restarted.	No Action Required.	Yes	No	No
10302	Information	Service Manager	Service Manager - CallPilot has been successfully restarted.	No Action Required.	Yes	No	No
10303	Information	Service Manager	Service Manager - IP Terminal Service (UTPS) has been successfully restarted.	No Action Required.	Yes	No	No

140 List of alarms

10305	Information	Service Manager	Service Manager - Voice over IP Gateway (feps) has been successfully restarted.	No Action Required.	Yes	No	No
10306	Information	Service Manager	Service Manager - Quality of Service Monitor (qmond) has been successfully restarted.	No Action Required.	Yes	No	No
10307	Information	Service Manager	Service Manager - Call Detail Recording Service (CDRService) has been successfully restarted.	No Action Required.	Yes	No	No
10308	Information	Service Manager	Service Manager - Voice Application Interface Service (ctiserver) has been successfully restarted.	No Action Required.	Yes	No	No
10309	Information	Service Manager	Service Manager - Modem Call Control (modemcc) has been successfully restarted.	No Action Required.	Yes	No	No

10310	Information	Service Manager	Service Manager - System Set Based Admin Feature9*8 (ssba) has been successfully restarted.	No Action Required.	Yes	No	No
10311	Information	Service Manager	Service Manager - Computer Telephony Service (Cte) has been successfully restarted.	No Action Required.	Yes	No	No
10312	Information	Service Manager	Service Manager - Line Monitor Service (lms) has been successfully restarted.	No Action Required.	Yes	No	No
10313	Information	Service Manager	Service Manager - Media Services Manager (Msm) has been successfully restarted.	No Action Required.	Yes	No	No
10314	Information	Service Manager	Service Manager - Media Path Server (mps) has been successfully restarted.	No Action Required.	Yes	No	No
10315	Information	Service Manager	Service Manager - Media Gateway Server (mgs) has been successfully restarted.	No Action Required.	Yes	No	No

142 List of alarms

10316	Information	Service Manager	Service Manager - Persistent Data Repository (Pdrd) has been successfully restarted.	No Action Required.	Yes	No	No
10317	Information	Service Manager	Service Manager - Keycode Service (cfserver) has been successfully restarted.	No Action Required.	Yes	No	No
10318	Information	Service Manager	Service Manager - Time Service (tmwservice) has been successfully restarted.	No Action Required.	Yes	No	No
10319	Information	Service Manager	Service Manager - Platform Status Monitor (psm) has been successfully restarted.	No Action Required.	Yes	No	No
10320	Information	Service Manager	Service Manager - Web Server (httpd) has been successfully restarted.	No Action Required.	Yes	No	No
10321	Information	Service Manager	Service Manager - On Box Management Framework (owcimomd) has been successfully restarted.	No Action Required.	Yes	No	No

10322	Information	Service Manager	Service Manager - Service Manager (monit) has been successfully restarted.	No Action Required.	Yes	No	No
10324	Information	Service Manager	Service Manager - IP Terminal Service (EchoServer) has been successfully restarted.	No Action Required.	Yes	No	No
10325	Information	Service Manager	Service Manager - IP Terminal Firmware upload Service (UftpServer) has been successfully restarted.	No Action Required.	Yes	No	No
10329	Information	Service Manager	Service Manager - Doorphone service (BCM_Doorphone) has been successfully restarted.	No Action Required.	Yes	No	No
10332	Information	Service Manager	Service Manager - IP Music Service (BcmAmp) has been successfully restarted.	No Action Required.	Yes	No	No
10333	Information	Service Manager	Service Manager - IP Music Service (ToneSrvr) has been successfully restarted.	No Action Required.	Yes	No	No

144 List of alarms

10906	Information	Startup Sequence	System Startup - Operating system and alarm subsystem available. Power LED = flashing green; Status LED = flashing yellow.	No Action Required.	Yes	No	No
10907	Information	Startup Sequence	System Startup - Telephony and Voicemail active. Power LED = flashing green; Status LED = flashing green.	No Action Required.	Yes	No	No
10908	Information	Startup Sequence	System Startup - Element Manager is available. Power LED = solid green; Status LED = flashing green.	No Action Required.	Yes	No	No
10909	Information	Startup Sequence	System Startup - Startup complete. Service Manager and Scheduling Services available. Power LED = solid green; Status LED = solid green.	No Action Required.	Yes	No	No



10916	Information	Startup Sequence	System Startup - Operating system and alarm subsystem available. Separate error alarm detected. Power LED = flashing green; Status LED = unchanged.	No Action Required.	Yes	No	No
10917	Information	Startup Sequence	System Startup - Telephony and Voicemail active. Separate error alarm detected. Power LED = flashing green; Status LED = unchanged.	No Action Required.	Yes	No	No
10918	Information	Startup Sequence	System Startup - Element Manager is available. Separate error alarm detected. Power LED = solid green; Status LED = unchanged.	No Action Required.	Yes	No	No

146 List of alarms

10919	Information	Startup Sequence	System Startup - Startup complete. Service Manager and Scheduling Services available. Separate error alarm detected. Power LED = solid green; Status LED = unchanged.	No Action Required.	Yes	No	No
11002	Information	Platform Status Monitor	Platform Status Monitor - Power recovered.	No Action Required. Recovery alarm for corresponding alarms 11200 and 11400.	Yes	No	No
11003	Information	Platform Status Monitor	Platform Status Monitor - Hard drive space recovered.	No Action Required. Recovery alarm for corresponding alarms 11201.	Yes	No	No
11004	Information	Platform Status Monitor	Platform Status Monitor - Memory recovered.	No Action Required. Recovery alarm for corresponding alarm 11202	Yes	No	No
11005	Information	Platform Status Monitor	Platform Status Monitor - CPU load recovered.	No Action Required. Recovery alarm for corresponding alarm 11203.	Yes	No	No

11006	Information	Platform Status Monitor	Platform Status Monitor - LAN recovered.	No Action Required. Recovery alarm for corresponding alarm 11204.	Yes	No	No
11011	Information	Platform Status Monitor	Platform Status Monitor - Local Temperature recovered.	No Action Required. Recovery alarm for corresponding alarms 11209 and 11405.	Yes	No	No
11012	Information	Platform Status Monitor	Platform Status Monitor - Remote Temperature recovered.	No Action Required. Recovery alarm for corresponding alarms 11210 and 11406.	Yes	No	No
11014	Information	Platform Status Monitor	Platform Status Monitor - Fan recovered.	No Action Required. Recovery alarm for corresponding alarms 11212 and 11408.	Yes	No	No
11015	Information	Platform Status Monitor	Platform Status Monitor - Router recovered.	No Action Required. Recovery alarm for corresponding alarm 11409.	Yes	No	No
11016	Information	Platform Status Monitor	Platform Status Monitor - OAM Port Link Up.	No Action Required. Recovery alarm for corresponding alarm 11214.	Yes	No	No
11017	Information	Platform Status Monitor	Platform Status Monitor - Customer LAN Port 1 Link Up.	No Action Required. Recovery alarm for corresponding alarm 11215.	Yes	No	No

148 List of alarms

11018	Information	Platform Status Monitor	Platform Status Monitor - Customer LAN Port 2 Link Up.	No Action Required. Recovery alarm for corresponding alarm 11216.	Yes	No	No
11019	Information	Platform Status Monitor	Platform Status Monitor - Customer LAN Port 3 Link Up.	No Action Required. Recovery alarm for corresponding alarm 11217.	Yes	No	No
11200	minor	Platform Status Monitor	Platform Status Monitor - failed to read Power.	Reboot system and if problem persists contact your local support group.	Yes	No	No
11201	major	Platform Status Monitor	Platform Status Monitor - Hard drive near capacity.	Contact local support group for assistance in recovering drive space.	Yes	Yes	Yes
11202	major	Platform Status Monitor	Platform Status Monitor - Memory near capacity.	Contact local support group for assistance in analyzing memory usage.	Yes	Yes	Yes

11203	minor	Platform Status Monitor	Platform Status Monitor - CPU load above threshold.	Use BCM Monitor for real-time view of CPU activity. Monitor for alarm 11005 to indicate CPU recovered. If problem persists, contact local support group.	Yes	No	No
11204	major	Platform Status Monitor	Platform Status Monitor - 1. rx_byte/sec greater than 50% of LAN%% speed, 2. tx_byte/sec greater than 50% of LAN%% speed, 3. rx_errors/sec of LAN%% > %%%, 4. tx_errors/sec of LAN%% > %%%, 5. rx_dropped/sec of LAN%% > %%%, 6. tx_dropped/sec of LAN%% > %%%	Verify that Customer LAN is performing as expected.	Yes	Yes	Yes

150 List of alarms

11021	information	Platform Status Monitor	Platform Status Monitor - Switch Control recovered.	No Action Required. Recovery alarm for corresponding alarms 11221 and 11301.	No	No	No
11022	information	Platform Status Monitor	Platform Status Monitor - Temperature Sensor 1 recovered.	No Action Required. Recovery alarm for corresponding alarms 11222 and 11302.	No	No	No
11023	information	Platform Status Monitor	Platform Status Monitor - Temperature Sensor 2 recovered.	No Action Required. Recovery alarm for corresponding alarms 11223 and 11303.	No	No	No
11024	information	Platform Status Monitor	Platform Status Monitor - Temperature Sensor 3 recovered.	No Action Required. Recovery alarm for corresponding alarms 11224 and 11304.	No	No	No
11025	information	Platform Status Monitor	Platform Status Monitor - Redundant Power Supply Module 1 recovered.	No Action Required. Recovery alarm for corresponding alarms 11225 and 11305.	No	No	No
11026	information	Platform Status Monitor	Platform Status Monitor - Redundant Power Supply Module 2 recovered.	No Action Required. Recovery alarm for corresponding alarms 11226 and 11306.	No	No	No

11027	information	Platform Status Monitor	Platform Status Monitor - Redundant Power Supply Fan 1 recovered.	No Action Required. Recovery alarm for corresponding alarms 11227 and 11307.	No	No	No
11028	information	Platform Status Monitor	Platform Status Monitor - Redundant Power Supply Fan 2 recovered.	No Action Required. Recovery alarm for corresponding alarms 11228 and 11308.	No	No	No
11209	major	Platform Status Monitor	Platform Status Monitor - Failed to read Local Temperature.	Reboot system and if problem reoccurs contact your local support group.	Yes	Yes	Yes
11210	major	Platform Status Monitor	Platform Status Monitor - Failed to read Remote Temperature.	Reboot system and if problem reoccurs contact your local support group.	Yes	Yes	Yes
11212	major	Platform Status Monitor	Platform Status Monitor - Fan Below Tolerance.	Check Fan operation as fan is apparently not working correctly. If alarm persists, replace fan.	Yes	Yes	Yes
11213	major	Platform Status Monitor	Platform Status Monitor - Failed to get Router status.	Check the router and if needed replace it.	Yes	Yes	Yes
11214	warning	Platform Status Monitor	Platform Status Monitor - OAM Port Link Down.	Check the OAM Port physical LAN connection	Yes	No	No

152 List of alarms

11215	warning	Platform Status Monitor	Platform Status Monitor - Customer LAN Port 1 Link Down.	Check the Customer LAN Port 1 physical LAN connection	Yes	No	No
11216	warning	Platform Status Monitor	Platform Status Monitor - Customer LAN Port 2 Link Down.	Check the Customer LAN Port 2 physical LAN connection	Yes	No	No
11217	warning	Platform Status Monitor	Platform Status Monitor - Customer LAN Port 3 Link Down.	Check the Customer LAN Port 3 physical LAN connection	Yes	No	No
11220	major	Platform Status Monitor	Platform Status Monitor - Failed to communicate with Switch Control.	Reboot system and if problem reoccurs contact your local support group.	No	No	No
11221	major	Platform Status Monitor	Platform Status Monitor - Temperature sensor 1 Out Of Range.	Reboot system and if problem reoccurs contact your local support group.	Yes	Yes	Yes
11222	major	Platform Status Monitor	Platform Status Monitor - Temperature sensor 2 Out Of Range.	Reboot system and if problem reoccurs contact your local support group.	Yes	Yes	Yes
11223	major	Platform Status Monitor	Platform Status Monitor - Temperature sensor 3 Out Of Range.	Reboot system and if problem reoccurs contact your local support group.	Yes	Yes	Yes



11224	major	Platform Status Monitor	Platform Status Monitor - Failed to read Redundant Supply Power Module 0.	Reboot system and if problem reoccurs contact your local support group.	Yes	Yes	Yes
11225	major	Platform Status Monitor	Platform Status Monitor - Failed to read Redundant Power Supply Module 1.	Reboot system and if problem reoccurs contact your local support group.	Yes	No	No
11226	major	Platform Status Monitor	Platform Status Monitor - Failed to read Redundant Power Supply Fan 1.	Reboot system and if problem reoccurs contact your local support group.	Yes	No	No
11227	major	Platform Status Monitor	Platform Status Monitor - Failed to read Redundant Power Supply Fan 2.	Reboot system and if problem reoccurs contact your local support group.	Yes	No	No
11250	major	Platform Status Monitor	Platform Status Monitor - The size of XXX Log file is greater than 16MB, XXX Log file will be deleted to recover / var/log partition.	Contact your local support group.	Yes	Yes	Yes

154 List of alarms

11300	minor	Platform Status Monitor	Platform Status Monitor - Power Rails Out Of Range.	Verify that external power is per operational limits. If alarm persists, contact your local support group.	Yes	No	No
11301	critical	Platform Status Monitor	Platform Status Monitor - Failed to read from Switch Control.	Device driver issue. Reboot system and if problem reoccurs contact your local support group.	No	No	No
11302	critical	Platform Status Monitor	Platform Status Monitor - Temperature sensor 1 reached critical tolerance, PSM gracefully reboots the system.	Check Fan operation and room temperatures as fan action has failed to maintain acceptable system temperatures.	Yes	Yes	Yes
11303	critical	Platform Status Monitor	Platform Status Monitor - Temperature sensor 2 reached critical tolerance, PSM gracefully reboots the system.	Check Fan operation and room temperatures as fan action has failed to maintain acceptable system temperatures.	Yes	Yes	Yes

11304	critical	Platform Status Monitor	Platform Status Monitor - Temperature sensor 3 reached critical tolerance, PSM gracefully reboots the system.	Check Fan operation and room temperatures as fan action has failed to maintain acceptable system temperatures.	Yes	Yes	Yes
11305	critical	Platform Status Monitor	Platform Status Monitor - Redundant Power Supply Module 1 Out Of Range.	Verify that external redundant power is per operational limits. If alarm persists, contact your local support group.	Yes	Yes	Yes
11306	critical	Platform Status Monitor	Platform Status Monitor - Redundant Power Supply Module 2 Out Of Range.	Verify that external redundant power is per operational limits. If alarm persists, contact your local support group.	Yes	Yes	Yes
11307	critical	Platform Status Monitor	Platform Status Monitor - Redundant Power Supply Fan 1 Out Of Range.	Check redundant power supply Fan0 operation as fan is apparently malfunctioning. If alarm persists, contact your local support group.	Yes	Yes	Yes

156 List of alarms

11308	critical	Platform Status Monitor	Platform Status Monitor - Redundant Power Supply Fan 2 Out Of Range.	Check redundant power supply Fan0 operation as fan is apparently malfunctioning. If alarm persists, contact your local support group.	Yes	Yes	Yes
11400	minor	Platform Status Monitor	Platform Status Monitor - Power %##% Failed.	Verify that external power is per operational limits. If alarm persists, contact your local support group.	Yes	No	No
11405	critical	Platform Status Monitor	Platform Status Monitor - Local Temperature above tolerance.	Check Fan operation and room temperature as fan action has failed to maintain acceptable system temperatures.	Yes	Yes	Yes
11406	critical	Platform Status Monitor	Platform Status Monitor - Remote Temperature above tolerance.	Check Fan operation and room temperature as fan action has failed to maintain acceptable system temperatures.	Yes	Yes	Yes

11408	critical	Platform Status Monitor	Platform Status Monitor - Fan speed is reading 0 for over 1 minute.	Check Fan operation as fan is apparently malfunctioning. If alarm persists, replace fan.	Yes	Yes	Yes
11409	critical	Platform Status Monitor	Platform Status Monitor - Router does not Exist.	Check Router operation as it is apparently malfunctioning. If alarm persists, replace router.	Yes	Yes	Yes
11502	critical	Platform Status Monitor	Platform Status Monitor - System out of Memory.	Contact your local support group for assistance in analyzing memory condition.	Yes	Yes	Yes
11503	information	Platform Status Monitor	Platform Status Monitor - Graceful Shutdown in progress. Power LED = solid green; Status LED = flash yellow.	No Action Required.	Yes	No	Yes
12001	major	Backup and Restore	Backup and Restore - Backup file could no be re-named.	Contact your local support group.	Yes	Yes	Yes
12002	major	Backup and Restore	Backup and Restore - Backup type is incorrect for its filesystem location.	Use a good backup to attempt the restore	Yes	Yes	Yes

158 List of alarms

12003	major	Backup and Restore	Backup and Restore - This backup type can not be restored.	Use a good backup to attempt the restore	Yes	Yes	Yes
12004	major	Backup and Restore	Backup and Restore - Internal error. Could not find associated connection definition.	Try backup again and if problem persists contact your local support group.	Yes	Yes	Yes
12005	major	Backup and Restore	Backup and Restore - Internal error. Could not create a file.	Try backup again and if problem persists contact your local support group.	Yes	Yes	Yes
12006	major	Backup and Restore	Backup and Restore - Internal error. Could not build the dynamic rule file.	Try backup again and if problem persists contact your local support group.	Yes	Yes	Yes
12007	major	Backup and Restore	Backup and Restore - Internal general error.	Try backup again and if problem persists contact your local support group.	Yes	Yes	Yes
12008	warning	Backup and Restore	Backup and Restore - Backup file is not recognizable.	Try a different backup file.	Yes	No	No
12009	major	Backup and Restore	Backup and Restore - Could not connect to the ftp site.	Check your connection configuration parameters and make sure FTP server is active	Yes	Yes	Yes

12010	minor	Backup and Restore	Backup and Restore - Could not authenticate with the ftp site.	Check your login credentials to the FTP server	Yes	No	No
12011	minor	Backup and Restore	Backup and Restore - Could not change ftp modes on the ftp site.	Check your FTP server configuration	Yes	No	No
12012	major	Backup and Restore	Backup and Restore - Could not send the file to the ftp site.	Check your connection configuration parameters and make sure FTP server is active	Yes	Yes	Yes
12013	major	Backup and Restore	Backup and Restore - Could not retrieve the file from the ftp site.	Check your connection configuration parameters and make sure FTP server is active	Yes	Yes	Yes
12014	major	Backup and Restore	Backup and Restore - Backup file integrity error.	Attempt another backup or restore.	Yes	Yes	Yes
12015	major	Backup and Restore	Backup and Restore - Backup file integrity error.	Attempt another backup or restore.	Yes	Yes	Yes
12016	warning	Backup and Restore	Backup and Restore - Backup is busy serving another request.	No Action Required.	Yes	No	No

160 List of alarms

12017	warning	Backup and Restore	Backup and Restore - File integrity error. Contents altered since creation.	Use a different backup file	Yes	No	No
12018	major	Backup and Restore	Backup and Restore - Internal error. Database could not be backed-up.	Attempt another backup and if problem persists contact your local support group	Yes	Yes	Yes
12019	warning	Backup and Restore	Backup and Restore - Backup file partially incompatible.	No Action Required.	Yes	No	No
12020	warning	Backup and Restore	Backup and Restore - Backup file partially incompatible.	No Action Required.	Yes	No	No
12021	major	Backup and Restore	Backup and Restore - Internal error. Could not shadow data.	Attempt another backup and if problem persists contact your local support group	Yes	Yes	Yes
12022	major	Backup and Restore	Backup and Restore - File is not recognizable. The signature is the wrong length.	Use a different backup file and if problem persists contact your local support group	Yes	Yes	Yes



12023	major	Backup and Restore	Backup and Restore - Backup file integrity error.	Use a different backup file and if problem persists contact your local support group	Yes	Yes	Yes
12024	major	Backup and Restore	Backup and Restore - Internal error. Compression incorrectly specified in configuration file.	Attempt another backup and if problem persists contact your local support group	Yes	Yes	Yes
12025	major	Backup and Restore	Backup and Restore - Internal error. Component in configuration file not recognized.	Attempt another backup and if problem persists contact your local support group	Yes	Yes	Yes
12026	major	Backup and Restore	Backup and Restore - Internal error. Unrecognized transfer mechanism.	Attempt another backup and if problem persists contact your local support group	Yes	Yes	Yes
12027	critical	Backup and Restore	Backup and Restore - File could not be copied to USB device.	Check the USB connection and flash device	Yes	Yes	Yes
12028	minor	Backup and Restore	Backup and Restore - File is incompatible with current software.	Use a backup from a supported software version	Yes	No	No

162 List of alarms

12029	major	Backup and Restore	Backup and Restore - Internal error. Could not restore the database.	Attempt another restore and if problem persists contact your local support group	Yes	Yes	Yes
12030	minor	Backup and Restore	Backup and Restore - File could not be transferred by sftp.	Check your login credentials to the SFTP server	Yes	No	No
12031	minor	Backup and Restore	Backup and Restore - File could not be transferred to the shared folder.	Check your login credentials to the shared folder	Yes	No	No
12032	major	Backup and Restore	Backup and Restore - Could not use the USB device.	Check the USB connection and space on the flash device	Yes	Yes	Yes
12033	minor	Backup and Restore	Backup and Restore - Could not detach the USB device.	Check the USB connection and flash device	Yes	No	No
12034	warning	Backup and Restore	Backup and Restore - Backup file is not recognizable.	Use a different backup file and if problem persists contact your local support group	Yes	No	No
12035	warning	Backup and Restore	Backup and Restore - Backup file is not recognizable.	Use a different backup file and if problem persists contact your local support group	Yes	No	No

12036	warning	Backup and Restore	Backup and Restore - Backup file is not recognizable.	Use a different backup file and if problem persists contact your local support group	Yes	No	No
12037	minor	Backup and Restore	Backup and Restore - Internal error.	Attempt another backup or restore and if problem persists contact your local support group	Yes	No	No
12038	minor	Backup and Restore	Backup and Restore - A backup file does not exist.	Attempt another backup or restore and if problem persists contact your local support group	Yes	No	No
12041	minor	Backup and Restore	Backup and Restore - Internal error.	Attempt another backup or restore and if problem persists contact your local support group	Yes	No	No
12059	major	Backup and Restore	Backup and Restore - The Voice Application Interface Service(ctiserver) service could not be restarted after a restore.	Restart the system and attempt another restore. If problem persists contact your local support group.	Yes	Yes	Yes

164 List of alarms

12202	Information	Backup and Restore	Backup and Restore - Onbox Backup/Log collection has completed.	No Action Required.	Yes	No	No
12203	Information	Backup and Restore	Backup and Restore - Backup/Log files have been successfully transferred off box.	No Action Required.	Yes	No	No
12204	Information	Backup and Restore	Backup and Restore - Restore has started.	No Action Required.	Yes	No	No
12205	Information	Backup and Restore	Backup and Restore - Restore has completed successfully.	No Action Required.	Yes	No	No
12206	Information	Backup and Restore	Backup and Restore - Restore has rebooted the system to complete its operation.	No Action Required.	Yes	No	No
13002	Information	UPS	UPS - Power failure.	Check local power connected to the system.	Yes	No	No
13003	Information	UPS	UPS - Running on UPS batteries.	Check local power connected to the system.	Yes	No	No
13004	warning	UPS	UPS - Battery power exhausted.	Check local power connected to the system.	Yes	No	No

13005	warning	UPS	UPS - Reached run time limit on batteries.	Check local power connected to the system.	Yes	No	No
13006	warning	UPS	UPS - Battery charge below low limit.	Check batteries in UPS and replace if needed.	Yes	No	No
13007	warning	UPS	UPS - Reached remaining time percentage limit on batteries.	No Action Required.	Yes	No	No
13008	warning	UPS	UPS - Failed to kill the power! Attempting a REBOOT!	Check USB connection to UPS.	Yes	No	No
13009	Information	UPS	UPS - Initiating system shutdown!.	System is going down due to power failures. Check local power connected to the system.	Yes	No	No
13010	Information	UPS	UPS - Power is back. UPS running on mains.	No Action Required.	Yes	No	No
13011	Information	UPS	UPS - Users requested to logoff.	No Action Required.	Yes	No	No
13012	major	UPS	UPS - Battery failure. Emergency.	Check batteries in UPS and replace if needed.	Yes	Yes	Yes
13013	major	UPS	UPS - UPS battery must be replaced.	Check batteries in UPS and replace if needed.	Yes	Yes	Yes

166 List of alarms

13014	Information	UPS	UPS - Remote shutdown requested.	No Action Required.	Yes	No	No
13015	major	UPS	UPS - Communications with UPS lost.	Check USB connection to UPS.	Yes	Yes	Yes
13016	Information	UPS	UPS - Communications with UPS restored.	No Action Required.	Yes	No	No
13017	Information	UPS	UPS - Self Test switch to battery.	No Action Required.	Yes	No	No
13018	Information	UPS	UPS - Self Test completed.	No Action Required.	Yes	No	No
13019	warning	UPS	UPS - Master not responding.	No Action Required.	Yes	No	No
13020	Information	UPS	UPS - Connect from master.	No Action Required.	Yes	No	No
13021	Information	UPS	UPS - Mains returned. No longer on UPS batteries.	No Action Required.	Yes	No	No
16001	Information	Configuration Change	Configuration Change - Configuration Change has occurred.	No Action Required.	No	No	No
17002	Information	System Set Based Admin	System Set Based Admin - UserId=X, Dn=Y, login success.	No Action Required.	No	No	No
17003	Information	System Set Based Admin	System Set Based Admin - UserId=X, Dn Y logged off.	No Action Required.	No	No	No
17004	Information	System Set Based Admin	System Set Based Admin - UserId=X, user account created successfully, Dn=Y.	No Action Required.	Yes	No	No

17005	Information	System Set Based Admin	System Set Based Admin - UserId=X, user account deleted successfully, Dn=Y.	No Action Required.	Yes	No	No
17006	Information	System Set Based Admin	System Set Based Admin - UserId=X, password changed successfully, Dn=Y.	No Action Required.	Yes	No	No
17007	Information	System Set Based Admin	System Set Based Admin - DHCP client enabled for eth1.	No Action Required.	Yes	No	No
17008	Information	System Set Based Admin	System Set Based Admin - DHCP client disabled for eth1.	No Action Required.	Yes	No	No
17009	Information	System Set Based Admin	System Set Based Admin - IP=%s, ip address changed successfully.	No Action Required.	Yes	No	No
17010	Information	System Set Based Admin	System Set Based Admin - MASK=%s, subnet mask changed successfully.	No Action Required.	Yes	No	No
17011	Information	System Set Based Admin	System Set Based Admin - Gateway=X, ip gateway changed successfully.	No Action Required.	Yes	No	No
17012	Information	System Set Based Admin	System Set Based Admin - Keycode validated.	No Action Required.	Yes	No	No

168 List of alarms

17013	Information	System Set Based Admin	System Set Based Admin - Reboot required.	No Action Required.	Yes	No	No
17015	Information	System Set Based Admin	System Set Based Admin - Modem Enabled/Disabled.	No Action Required.	Yes	No	No
17100	warning	System Set Based Admin	System Set Based Admin - System Set Based Admin general warning alarm.	Problem exists using System Set Based Admin. If problem persists contact your local support group.	Yes	No	No
17111	warning	System Set Based Admin	System Set Based Admin - UserID = X, password changed failed.	Log back into System Set based admin to verify change. If problem persists contact your local support group.	Yes	No	No
17112	warning	System Set Based Admin	System Set Based Admin - UserID = X, user account creation failed.	Log back into System Set based admin to verify change. If problem persists contact your local support group.	Yes	No	No



17113	warning	System Set Based Admin	System Set Based Admin - UserID = X, user account deletion failed.	Log back into System Set based admin to verify change. If problem persists contact your local support group.	Yes	No	No
17120	warning	System Set Based Admin	System Set Based Admin - Key code activation failed.	Log back into System Set based admin to verify change. If problem persists contact your local support group.	Yes	No	No
17121	warning	System Set Based Admin	System Set Based Admin - Key code set failed.	Log back into System Set based admin to verify key-code. If problem persists contact your local support group.	Yes	No	No
17130	warning	System Set Based Admin	System Set Based Admin - Get modem PDR value failed.	Log back into System Set based admin to verify modem settings. If problem persists contact your local support group.	Yes	No	No

170 List of alarms

17131	warning	System Set Based Admin	System Set Based Admin - Set modem PDR value failed.	Log back into System Set based admin to verify modem settings. If problem persists contact your local support group.	Yes	No	No
17140	warning	System Set Based Admin	System Set Based Admin - LAN ip address change failed, ip = X.	Log back into System Set based admin to verify change. If problem persists contact your local support group.	Yes	No	No
17141	warning	System Set Based Admin	System Set Based Admin - LAN subnet mask change failed, mask = X.	Log back into System Set based admin to verify change. If problem persists contact your local support group.	Yes	No	No
17142	warning	System Set Based Admin	System Set Based Admin - LAN Gateway change failed, gateway = X.	Log back into System Set based admin to verify change. If problem persists contact your local support group.	Yes	No	No

17200	critical	System Set Based Admin	System Set Based Admin - System Set Based Admin general critical alarm.	Problem exists using System Set Based Admin. If problem persists contact your local support group.	Yes	Yes	Yes
18001	Major	BootLoader	Self test was unable to provide results. Flash memory may be malfunctioning	Contact your local support group	Yes	Yes	Yes
18002	Major	BootLoader	RAM size is less than expected	Contact your local support group	Yes	Yes	Yes
18003	Major	BootLoader	Flash size is less than expected	Contact your local support group	Yes	Yes	Yes
18004	Critical	BootLoader	System initialization failed	Contact your local support group	Yes	Yes	Yes
18005	Minor	BootLoader	Network initialization failed	Contact your local support group	Yes	No	No
18006	Minor	BootLoader	Ethernet MAC addresses not found	Contact your local support group	Yes	No	No
18007	Critical	BootLoader	Hard drive initialization failed	Contact your local support group	Yes	Yes	Yes
19002	critical	Startup Profile	Startup Profile - Startup Profile had 1 or more errors when trying to apply.	Check log file on USB device.	Yes	Yes	Yes
19010	Information	Startup Profile	Startup Profile - Startup Profile completed successfully.	No Action Required.	Yes	No	No
19101	warning	Startup Profile	Startup Profile - Startup Profile failed to apply because previous log file exists on USB device.	Delete existing log file on USB to continue.	Yes	No	No
21100	critical	DSP Manager	DSP Manager - DSP failed to initialize.	Reboot the system. If problem persists contact your local support group.	Yes	Yes	Yes

172 List of alarms

30100	major	System Authentication	System Authentication - User Locked out.	Check user account for potential security issues.	Yes	Yes	Yes
30101	information	System Authentication	System Authentication - User Lockout ended.	No Action Required.	Yes	No	No
30200	information	System Authentication	System Authentication - User logon User=X Host=Y Comp=Z.	No Action Required.	No	No	No
30201	information	System Authentication	System Authentication - User logoff User=X Comp=SBA.	No Action Required.	No	No	No
30202	minor	System Authentication	System Authentication - User failed to login User=X Host=Y Comp=Z.	Monitor user activity for lockout condition. If concerned, check "Last successful login" timestamp on View by Accounts panel.	Yes	No	No
30203	information	System Authentication	System Authentication - User logon User=X Host=Y Comp=WWW.	No Action Required.	Yes	No	No
30300	information	System Authentication	System Authentication - Account created.	No Action Required.	Yes	No	No
30301	information	System Authentication	System Authentication - Account updated.	No Action Required.	Yes	No	No
30302	information	System Authentication	System Authentication - Account password changed.	No Action Required.	Yes	No	No
30303	information	System Authentication	System Authentication - Account enabled.	No Action Required.	Yes	No	No
30304	information	System Authentication	System Authentication - Account deleted User=X Comp=Y.	No Action Required.	Yes	No	No

30400	information	System Authentication	System Authentication - Group Created.	No Action Required.	Yes	No	No
30401	information	System Authentication	System Authentication - Group member added.	No Action Required.	Yes	No	No
30402	information	System Authentication	System Authentication - Group member removed.	No Action Required.	Yes	No	No
30403	information	System Authentication	System Authentication - Group Deleted.	No Action Required.	Yes	No	No
30404	information	System Authentication	System Authentication - Group permissions modified.	No Action Required.	Yes	No	No
31006	critical	Keycodes	Keycodes - invalid license file.	Restore licensing file or enter keycodes again.	Yes	Yes	Yes
31007	critical	Keycodes	Keycodes - unknown license file status.	Restore licensing file or enter keycodes again.	Yes	Yes	Yes
31019	warning	Keycodes	Keycodes - failed to find component (<component handle>).	Ensure component is running properly and if problem persists contact your local support group.	Yes	No	No
31045	critical	Keycodes	Keycodes - failed to open file.	Restore licensing file or enter keycodes again.	Yes	Yes	Yes
31052	critical	Keycodes	Keycodes - failed to open license file.	Restore licensing file or enter keycodes again.	Yes	Yes	Yes

174 List of alarms

31055	critical	Keycodes	Keycodes - failed to read system id.	Reboot the system and if problem persists contact your local support group.	Yes	Yes	Yes
31056	critical	Keycodes	Keycodes - cannot find system id tag.	Restore licensing file or enter keycodes again.	Yes	Yes	Yes
31057	critical	Keycodes	Keycodes - failed to read sequence number.	Restore licensing file or enter keycodes again.	Yes	Yes	Yes
31058	critical	Keycodes	Keycodes - cannot find sequence tag.	Restore licensing file or enter keycodes again.	Yes	Yes	Yes
31059	critical	Keycodes	Keycodes - failed to read key type.	Restore licensing file or enter keycodes again.	Yes	Yes	Yes
31062	critical	Keycodes	Keycodes - failed to read key code <key-code size>.	Restore licensing file or enter keycodes again.	Yes	Yes	Yes
31063	critical	Keycodes	Keycodes - failed to find key code.	Restore licensing file or enter keycodes again.	Yes	Yes	Yes
31067	critical	Keycodes	Keycodes - failed to find component for feature.	Ensure component is running properly and if problem persists contact your local support group.	Yes	Yes	Yes

31068	critical	Keycodes	Keycodes - invalid data range for feature (<feature code> <feature data>).	Contact your local support group.	Yes	Yes	Yes
31079	critical	Keycodes	Keycodes - wrong system id.	Check the system ID in your licensing configuration.	Yes	Yes	Yes
31089	critical	Keycodes	Keycodes - wrong sequence number.	Check the sequence number in your licensing configuration.	Yes	Yes	Yes
31130	warning	Keycodes	Keycodes - Keycode could not be activated.	Check requirements for the keycode and if the problem persists contact your local support group.	Yes	No	No
31250	warning	Software Updates	The R3 factory image upgrade patch has not been installed. Performing a level 2 reset will downgrade the system to a non R3 software level.	Apply the R3 factory image upgrade patch	Yes	Yes	No
31251	major	Keycodes	Keycodes - invalid software load detected and keycode processing stopped.	Include software upgrade keycode in the applying keycode file.	No	Yes	Yes
40002	information	Media Services Manager	MSM - DSP initialized.	No Action Required.	Yes	No	No

176 List of alarms

40003	critical	Media Services Manager	MSM - Unable to communicate with DSP.	Reboot system and if problem persists contact your local support group.	Yes	Yes	Yes
40004	warning	Media Services Manager	MSM - DSP audit failed.	Contact your local support group.	Yes	No	No
40005	critical	Media Services Manager	MSM - DSP reset.	If alarm 40002 proceeds this then no action required otherwise contact your local support group.	Yes	Yes	Yes
41001	major	CTE	CTE - Cte table corruption.	Contact your local support group.	Yes	Yes	Yes
41002	major	CTE	CTE - Unsupported KSU.	Restart system and if problem persists contact your local support group.	Yes	Yes	Yes
41003	major	CTE	CTE - Incorrect state index in the state machine.	Contact your local support group.	Yes	Yes	Yes
41004	warning	CTE	CTE - Error replying to licensing process.	Check your licensing information.	Yes	No	No
41005	minor	CTE	CTE - Error getting feature from list in licensing process.	Check your licensing information.	Yes	No	No
41006	warning	CTE	CTE - Error processing Data Status in licesning process.	Check your licensing information.	Yes	No	No



42200	warning	Call Detail Recording Transfer	CDR Transfer minor error.	Check your configuration parameters.	Yes	No	No
42500	critical	Call Detail Recording Transfer	CDR Transfer initialization error.	Contact your local support group.	Yes	Yes	Yes
42501	critical	Call Detail Recording Transfer	CDR Transfer processing error.	Check your configuration parameters and if problem persists contact your local support group.	Yes	Yes	Yes
42502	critical	Call Detail Recording Transfer	CDR Transfer working error.	Check your configuration parameters and if problem persists contact your local support group.	Yes	Yes	Yes
43002	warning	Voice CTI	Voice CTI no voice channels allocated.	Contact your local support group.	Yes	No	No
43003	critical	Voice CTI	Voice CTI unable to register with MSM.	Contact your local support group.	Yes	Yes	Yes
43004	critical	Voice CTI	Voice CTI subcomponent failure.	Contact your local support group.	Yes	Yes	Yes
43005	critical	Voice CTI	Voice CTI software error.	Contact your local support group.	Yes	Yes	Yes
43006	warning	Voice CTI	Voice CTI application did not register properly.	Contact your local support group.	Yes	No	No

178 List of alarms

43008	information	Voice CTI	Voice CTI - More than 20 percent voice file space available.	No Action Required.	Yes	No	No
43009	warning	Voice CTI	Voice CTI - Less than 20 percent voice file space available.	Check voice mailboxes for excessive messages and if problem persists contact your local support group.	Yes	No	No
43010	critical	Voice CTI	Voice CTI - Less than 5 percent voice file space available.	Check voice mailboxes for excessive messages and if problem persists contact your local support group.	Yes	Yes	Yes
43017	warning	Voice CTI	Insufficient DSP resources for FAX.	If the problem persists, increase the number of DSP on the system.	Yes	No	No
43018	warning	Voice CTI	Insufficient DSP resources for VOICE.	If the problem persists, increase the number of DSP on the system.	Yes	No	No
43019	warning	Voice CTI	Insufficient DSP resources for MO-DEM.	If the problem persists, increase the number of DSP on the system.	Yes	No	No

50001	critical	Unistim Terminal Proxy Server	The UTPS cannot determine whether or not the BCM is running in SRG mode. Without that information, the UTPS cannot continue: aborting with error << errorCode.	Contact your local support group.	Yes	Yes	Yes
50002	critical	Unistim Terminal Proxy Server	The UTPS cannot determine whether or not the BCM is running in SRG mode. Without that information, the UTPS cannot continue: aborting with error << errorCode.	Contact your local support group.	Yes	Yes	Yes
50003	critical	Unistim Terminal Proxy Server	UTPS failed to initialize itself because of an internal error. The UTPS is aborting.	Contact your local support group.	Yes	Yes	Yes

180 List of alarms

50004	critical	Unistim Terminal Proxy Server	UTPS has determined that the SRG keycode has been applied but the SRG process is not running properly. UTPS is aborting with error << error-Code.	Contact your local support group.	Yes	Yes	Yes
50005	critical	Unistim Terminal Proxy Server	UTPS has determined that the SRG process is not running but cannot determine whether or not the SRG key-code has been applied - the UTPS cannot continue without that information; aborting with error << error-Code.	Contact your local support group.	Yes	Yes	Yes
50006	critical	Unistim Terminal Proxy Server	UTPS failed to establish a link to the SRG process. Aborting with error << errorCode.	Contact your local support group.	Yes	Yes	Yes

50007	critical	Unistim Terminal Proxy Server	UTPS opened a link with the SRG process but failed to get the SRG key-code information: Aborting with error << errorCode.	Contact your local support group.	Yes	Yes	Yes
50008	critical	Unistim Terminal Proxy Server	UTPS has lost its link to the SRG process and can no longer continue - terminating.	Contact your local support group.	Yes	Yes	Yes
50009	critical	Unistim Terminal Proxy Server	UTPS waited for SRG process to supply SRG key-code information but no response was received - terminating.	Contact your local support group.	Yes	Yes	Yes
50010	critical	Unistim Terminal Proxy Server	UTPS failed to create socket on UDP port << utpsPort << . Terminating with error << errorCode.	Contact your local support group.	Yes	Yes	Yes

182 List of alarms

---

50011	critical	Unistim Terminal Proxy Server	UTPS failed to retrieve vital information about the network adaptors present on the BCM. UTPS is aborting with error << errorCode.	Contact your local support group.	Yes	Yes	Yes
50012	critical	Unistim Terminal Proxy Server	The published IP address has just been changed - the UTPS will restart and start using the new published IP address.	Contact your local support group.	Yes	Yes	Yes
50013	critical	Unistim Terminal Proxy Server	UTPS failed to obtain the detailed terminal list from the core telephony engine. The detailed error description is: << detailedString.	Contact your local support group.	Yes	Yes	Yes

50014	critical	Unistim Terminal Proxy Server	UTPS failed to retrieve vital information about the UDP socket used to communicate with IP sets. terminating with error << error-Code.	Contact your local support group.	Yes	Yes	Yes
50015	critical	Unistim Terminal Proxy Server	The UTPS couldn't find the network adaptor that is bound to the published IP address - aborting.	Contact your local support group.	Yes	Yes	Yes
50050	critical	Unistim Terminal Proxy Server	The UTPS experienced an internal error preventing it from properly handling incoming connection requests from IP sets - aborting.	Contact your local support group.	Yes	Yes	Yes
50060	critical	Unistim Terminal Proxy Server	An exception was caught trying to initialize the EPF layer - aborting.	Contact your local support group.	Yes	Yes	Yes

184 List of alarms

50061	critical	Unistim Terminal Proxy Server	UTPS failed to initialize the EPF layer. Aborting with error << errorCode.	Contact your local support group.	Yes	Yes	Yes
50062	critical	Unistim Terminal Proxy Server	An unidentified fatal error occurred inside EPF layer - terminating.	Contact your local support group.	Yes	Yes	Yes
50064	critical	Unistim Terminal Proxy Server	The Media Path Management subsystem unexpectedly became offline - terminating.	Contact your local support group.	Yes	Yes	Yes
50065	critical	Unistim Terminal Proxy Server	UTPS failed to initialize the EPF layer - terminating with MPSMI return code of << errorCode.	Contact your local support group.	Yes	Yes	Yes
50101	major	Unistim Terminal Proxy Server	UTPS is unable to initialize the NNU security interface. << errorCode.	Contact your local support group.	Yes	Yes	Yes
50102	major	Unistim Terminal Proxy Server	ERROR: Application::Run returned << errorCode.	Contact your local support group.	Yes	Yes	Yes
50103	major	Unistim Terminal Proxy Server	Unable to update the feature table in the PDR (error << ret <<).	Contact your local support group.	Yes	Yes	Yes



50104	major	Unistim Terminal Proxy Server	tPerDNConfiguration::ListenerDn-Changed could not find entry for DN << oldDn.	Contact your local support group.	Yes	Yes	Yes
50105	major	Unistim Terminal Proxy Server	Attempting to save jitter for the invalid DN of << dn.	Contact your local support group.	Yes	Yes	Yes
50106	major	Unistim Terminal Proxy Server	Attempting to save codec for the invalid DN of << dn.	Contact your local support group.	Yes	Yes	Yes
50108	major	Unistim Terminal Proxy Server	Error << errorCode << writing advertisement logo \ << logo<< \ to PDR.	Contact your local support group.	Yes	Yes	Yes
50109	major	Unistim Terminal Proxy Server	Error << errorCode << changing registration flag in registry.	Contact your local support group.	Yes	Yes	Yes
50110	major	Unistim Terminal Proxy Server	Error << errorCode << changing global password flag in registry.	Contact your local support group.	Yes	Yes	Yes
50111	major	Unistim Terminal Proxy Server	Error << errorCode << attempting to store registration password in registry.	Contact your local support group.	Yes	Yes	Yes

186 List of alarms

50112	major	Unistim Terminal Proxy Server	Error << errorCode << changing AutoAssignDN flag in registry.	Contact your local support group.	Yes	Yes	Yes
50113	major	Unistim Terminal Proxy Server	Failed to send message; cannot process OAM command.	Contact your local support group.	Yes	Yes	Yes
50114	major	Unistim Terminal Proxy Server	terminalIdentifier << Could not register terminal with UNIS- timIOHandler.	Contact your local support group.	Yes	Yes	Yes
50115	major	Unistim Terminal Proxy Server	terminalIdentifier << : No public media address available - EchoServer may be down or misconfigured.	Contact your local support group.	Yes	Yes	Yes
50116	major	Unistim Terminal Proxy Server	failed to insert << element << in m_mapInstantiated Terminals.	Contact your local support group.	Yes	Yes	Yes
50117	major	Unistim Terminal Proxy Server	Firmware download session rejected. Reason is << rejectionCause.	Contact your local support group.	Yes	Yes	Yes

50118	major	Unistim Terminal Proxy Server	UTPS has failed to authenticate the supplied user ID due to an internal error - error code = << errorCode.	Contact your local support group.	Yes	Yes	Yes
50119	major	Unistim Terminal Proxy Server	UTPS has failed to authenticate the supplied user ID due to an internal error - error code = << errorCode.	Contact your local support group.	Yes	Yes	Yes
50120	major	Unistim Terminal Proxy Server	Attempt to Hot Desk << dnToHighjack << from << hijackerDn << has failed [Debug information << sessionId << << errorCode << ].	Contact your local support group.	Yes	Yes	Yes

188 List of alarms

50121	major	Unistim Terminal Proxy Server	Attempt to Hot Desk << dnToHighjack << from << HighjackerDn << has failed because 'stand-by Hot Desking service' could be started [Debug information << sessionId << << errorCode << ].	Contact your local support group.	Yes	Yes	Yes
50122	major	Unistim Terminal Proxy Server	Hot Desking Session initiated by << highjackerDn << has failed to start with internal error.	Contact your local support group.	Yes	Yes	Yes
50123	major	Unistim Terminal Proxy Server	HotDesking session termination between << Dn1 << and << Dn2 << failed : internal data structure out of synch.	Contact your local support group.	Yes	Yes	Yes

50124	major	Unistim Terminal Proxy Server	HotDesking session termination between << Dn1 << and << Dn1 << failed : cannot find standby Hot Desking session.	Contact your local support group.	Yes	Yes	Yes
50125	major	Unistim Terminal Proxy Server	Lost Connection to SRG.	Contact your local support group.	Yes	Yes	Yes
50192	major	Unistim Terminal Proxy Server	AppFwCriticalSection::init osCreateEvent rc = << errorCode.	Contact your local support group.	Yes	Yes	Yes
50193	major	Unistim Terminal Proxy Server	AppFwCriticalSection::init osCreateEvent rc = << errorCode.	Contact your local support group.	Yes	Yes	Yes
50194	major	Unistim Terminal Proxy Server	AppFwCriticalSection::MessageToSelf osReceiveError << errorCode.	Contact your local support group.	Yes	Yes	Yes
50195	major	Unistim Terminal Proxy Server	AppFwCriticalSection::Acquire osReceiveError << errorCode.	Contact your local support group.	Yes	Yes	Yes
50196	major	Unistim Terminal Proxy Server	In Application::InitializationComplete but NnuServiceInitialized returned << errorCode << APPLICATION WILL BE SHUT DOWN.	Contact your local support group.	Yes	Yes	Yes

190 List of alarms

50197	major	Unistim Terminal Proxy Server	Application::Run caught unspecified exception: FORCING EMERGENCY SHUTDOWN.	Contact your local support group.	Yes	Yes	Yes
50198	major	Unistim Terminal Proxy Server	Application::Run caught exception: << exceptionType << FORCING EMERGENCY SHUTDOWN.	Contact your local support group.	Yes	Yes	Yes
50300	information	Unistim Terminal Proxy Server	** Running the DEBUG version of UTPS, version << UtpsVersion.	No Action Required.	Yes	No	No
50301	information	Unistim Terminal Proxy Server	** Running the RELEASE version of UTPS, version << UtpsVersion.	No Action Required.	No	No	No
50302	information	Unistim Terminal Proxy Server	BCM running in SRG/BCM mode.	No Action Required.	Yes	No	No
50303	information	Unistim Terminal Proxy Server	Terminal << dn << is being deregistered from OAM.	No Action Required.	Yes	No	No

50304	information	Unistim Terminal Proxy Server	The IP Terminal at << IpAddress << is NOT configured to connect to the BCM's published IP address - please correct the IP Terminal's configuration.	No Action Required.	Yes	No	No
50305	information	Unistim Terminal Proxy Server	System running in SRG mode.	No Action Required.	Yes	No	No
50306	information	Unistim Terminal Proxy Server	System NOT running in SRG mode.	No Action Required.	No	No	No
50307	information	Unistim Terminal Proxy Server	SRG Connection Re-established.	No Action Required.	Yes	No	No
50308	information	Unistim Terminal Proxy Server	Terminal << dn << : firmware version being upgraded from << oldFirmwareVersion << to << newFirmwareVersion.	No Action Required.	Yes	No	No

192 List of alarms

50501	information	Unistim Terminal Proxy Server	Packet Loss Violation Cleared: <>, near DN: <>, source IP: <>, source port: <>, destination IP: <>, destination port: <>, cT <>,eT <>,nLR <>,dR <>,bD <>,bL <>,gD <>,gL <>, eSD <>,aNL < >,aSP <>,rTT <>.	No Action Required.	Yes	Yes	No
50502	warning	Unistim Terminal Proxy Server	Packet Loss Violation Warning: <>, near DN: <>, source IP: <>, source port: <>, destination IP: <>, destination port: <>, cT <>,eT <>,nLR <>,dR <>,bD <>,bL <>,gD <>,gL <>, eSD <>,aNL < >,aSP <>,rTT <>.	No Action Required.	Yes	Yes	No



50503	minor	Unistim Terminal Proxy Server	Packet Loss Violation Unacceptable <>, near DN: <>, source IP: <>, source port: <>, destination IP: <>, destination port: <>, cT <>,eT <>,nLR <>,dR <>,bD <>,bL <>,gD <>,gL <>, eSD <>,aNL < >,aSP <>,rTT <>.	No Action Required.	Yes	Yes	No
50504	information	Unistim Terminal Proxy Server	Inter Arrival Jitter Violation Cleared: <>, near DN: <>, source IP: <>, source port: <>, destination IP: <>, destination port: <>, cT <>,eT <>,nLR <>,dR <>,bD <>,bL <>,gD <>,gL <>, eSD <>,aNL < >,aSP <>,rTT <>.	No Action Required.	Yes	Yes	No

194 List of alarms

50505	warning	Unistim Terminal Proxy Server	Inter Arrival Jitter Violation Warning: <>, near DN: <>, source IP: <>, source port: <>, destination IP: <>, destination port: <>, cT <>,eT <>,nLR <>,dR <>,bD <>,bL <>,gD <>,gL <>, eSD <>,aNL < >,aSP <>,rTT <>.	No Action Required.	Yes	Yes	No
50506	minor	Unistim Terminal Proxy Server	Inter Arrival Jitter Violation Unacceptable: <>, near DN: <>, source IP: <>, source port: <>, destination IP: <>, destination port: <>, cT <>,eT <>,nLR <>,dR <>,bD <>,bL <>,gD <>,gL <>, eSD <>,aNL < >,aSP <>,rTT <>.	No Action Required.	Yes	Yes	No

50507	information	Unistim Terminal Proxy Server	Round Trip Delay Violation Cleared: <>, near DN: <>, source IP: <>, source port: <>, destination IP: <>, destination port: <>, cT <>,eT <>,nLR <>,dR <>,bD <>,bL <>,gD <>,gL <>, eSD <>,aNL < >,aSP <>,rTT <>.	No Action Required.	Yes	Yes	No
50508	warning	Unistim Terminal Proxy Server	Round Trip Delay Violation Warning: <>, near DN: <>, source IP: <>, source port: <>, destination IP: <>, destination port: <>, cT <>,eT <>,nLR <>,dR <>,bD <>,bL <>,gD <>,gL <>, eSD <>,aNL < >,aSP <>,rTT <>.	No Action Required.	Yes	Yes	No

196 List of alarms

50509	minor	Unistim Terminal Proxy Server	Round Trip Delay Violation Unacceptable: <>, near DN: <>, source IP: <>, source port: <>, destination IP: <>, destination port: <>, cT <>,eT <>,nLR <>,dR <>,bD <>,bL <>,gD <>,gL <>, eSD <>,aNL < >,aSP <>,rTT <>.	No Action Required.	Yes	Yes	No
50510	information	Unistim Terminal Proxy Server	Listening R Factor Violation Cleared: <>, near DN: <>, source IP: <>, source port: <>, destination IP: <>, destination port: <>, cT <>,eT <>,nLR <>,dR <>,bD <>,bL <>,gD <>,gL <>, eSD <>,aNL < >,aSP <>,rTT <>.	No Action Required.	Yes	Yes	No

50511	warning	Unistim Terminal Proxy Server	Listening R Factor Violation Warning: <>, near DN: <>, source IP: <>, source port: <>, destination IP: <>, destination port: <>, cT <>,eT <>,nLR <>,dR <>,bD <>,bL <>,gD <>,gL <>, eSD <>,aNL < >,aSP <>,rTT <>.	No Action Required.	Yes	Yes	No
51010	warning	VoIP Gateway	VoIP Gateway configuration parameters not found.	Restore a known good backup into the system . If the problem persists contact your local support group.	Yes	No	No
51014	information	VoIP Gateway	VoIP Gateway succeeded to ping gatekeeper address.	No Action Required.	Yes	No	No

198 List of alarms

51015	warning	VoIP Gateway	VoIP Gateway failed to ping gatekeeper address.	Check that the gatekeeper is configured correctly, and is accessible. The system will keep trying to make contact with the gatekeeper at 3 minute intervals.	Yes	No	No
51016	warning	VoIP Gateway	VoIP Gateway remote gateway mismatch.	Verify the remote gateway is supported for interoperability.	Yes	No	No
51020	critical	VoIP Gateway	VoIP Gateway failed to initialize h.323 stack.	Contact your local support group.	Yes	Yes	Yes
51024	major	VoIP Gateway	VoIP Gateway can't communicate with QoS monitor.	Check the status of the QoS monitor in Element Manager.	Yes	Yes	Yes
51100	major	VoIP Gateway	VoIP Gateway rejected call setup attempt from DN <DN> to DN <DN>: <reason>.	Ensure the codecs are set-up properly in the system. If problem persists use BCM monitor to trace an unsuccessful call and contact your local support group.	Yes	Yes	Yes

51101	major	VoIP Gateway	VoIP Gateway dropped connected call from DN <DN> to DN <DN>: <reason>.	The call has dropped, possibly due to incompatible codecs, network errors, or protocol problems. If problem persists contact your local support group.	Yes	Yes	Yes
51901	critical	VoIP Gateway	VoIP Gateway serious system error.	Contact your local support group.	Yes	Yes	Yes
51903	critical	VoIP Gateway	VoIP Gateway exception error.	Contact your local support group.	Yes	Yes	Yes
51904	critical	VoIP Gateway	VoIP Gateway exception error.	Contact your local support group.	Yes	Yes	Yes
52000	critical	Media Path Server	MPS unable to allocate memory. MPS service aborted.	Reboot system and if problem persists contact your local support group.	Yes	Yes	Yes
52001	critical	Media Path Server	MPS unable to initialize MPSMI. MPS service aborted.	Contact your local support group.	Yes	Yes	Yes
52002	critical	Media Path Server	MPS unable to connect to MSM. MPS service aborted.	Contact your local support group.	Yes	Yes	Yes
52003	critical	Media Path Server	MPS unable to open FUMP channels. MPS service aborted.	Contact your local support group.	Yes	Yes	Yes
52004	critical	Media Path Server	MPS FUMP channel not ready. MPS service aborted.	Contact your local support group.	Yes	Yes	Yes

## 200 List of alarms

52005	critical	Media Path Server	MPS reset by network manager.	Contact your local support group.	Yes	Yes	Yes
52006	critical	Media Path Server	MPS received connection lost from MSM. MPS service aborted.	Contact your local support group.	Yes	Yes	Yes
52007	critical	Media Path Server	MPS unable to create event. MPS service failed to start.	Contact your local support group.	Yes	Yes	Yes
52008	critical	Media Path Server	MPS unable to initialize NNU messaging framework.	Contact your local support group.	Yes	Yes	Yes
52009	critical	Media Path Server	MPS unable to initialize message loop thread.	Contact your local support group.	Yes	Yes	Yes
52013	warning	Media Path Server	MPS codec incompatible, call dropped.	Contact your local support group.	Yes	No	No
52014	warning	Media Path Server	MPS endpoint registration failed.	Contact your local support group.	Yes	No	No
53000	critical	Media Gateway Server	MGS Exception software error.	Contact your local support group.	Yes	Yes	Yes
53001	critical	Media Gateway Server	MGS shutting down due to gateway creation failure.	Contact your local support group.	Yes	Yes	Yes
53002	critical	Media Gateway Server	MGS shutting down due to gateway initialization error.	Contact your local support group.	Yes	Yes	Yes
53003	critical	Media Gateway Server	MGS shutting down due to a fatal error.	Contact your local support group.	Yes	Yes	Yes
53004	critical	Media Gateway Server	MGS shutting down due to MSM communication failure.	Contact your local support group.	Yes	Yes	Yes
53005	critical	Media Gateway Server	MGS shutting down due to MPS communication failure.	Contact your local support group.	Yes	Yes	Yes



53006	critical	Media Gateway Server	MGS shutting down due to resource limits query failure.	Contact your local support group.	Yes	Yes	Yes
53007	critical	Media Gateway Server	MGS shutting down due to configuration query failure.	Contact your local support group.	Yes	Yes	Yes
53008	critical	Media Gateway Server	MGS MediaTransport Received bad ports: <port1> <port2>.	Contact your local support group.	Yes	Yes	Yes
53009	critical	Media Gateway Server	MGS MediaTransport Codec and/or frames per packet mismatch <details>.	Contact your local support group.	Yes	Yes	Yes
53010	critical	Media Gateway Server	MGS MediaTransport: Transport mismatch <details>.	Contact your local support group.	Yes	Yes	Yes
53011	critical	Media Gateway Server	MGS MsmProxy:: <interface> returned error <error>.	Contact your local support group.	Yes	Yes	Yes
53012	critical	Media Gateway Server	MGS <entity>:: <interface> returned error <error>.	Contact your local support group.	Yes	Yes	Yes
53018	critical	Media Gateway Server	MGS ResourceMediaController::<OID=<oid>> DSP Task Lost.	Contact your local support group.	Yes	Yes	Yes
53019	information	Media Gateway Server	MGS Shutting down due to IP address change.	No Action Required as service manager will restart.	Yes	No	No
53020	warning	Media Gateway Server	Insufficient DSP resources for G.711.	If the problem persists, increase the number of DSP on the system.	Yes	Yes	Yes
53021	warning	Media Gateway Server	Insufficient DSP resources for G.729.	If the problem persists, increase the number of DSP on the system.	Yes	Yes	Yes

## 202 List of alarms

53022	warning	Media Gateway Server	Insufficient DSP resources for T.38.	If the problem persists, increase the number of DSP on the system.	Yes	Yes	Yes
56003	major	IP Telephony Provider	IP Telphony Provider fatal error was detected.	Contact your local support group.	Yes	Yes	Yes
56004	minor	IP Telephony Provider	IP Telphony Provider error was detected.	Contact your local support group.	Yes	No	No
56005	major	IP Telephony Provider	IP Telphony Provider software exception.	Contact your local support group.	Yes	Yes	Yes
56006	minor	IP Telephony Provider	IP Telphony Provider shutting down due to fatal error.	Contact your local support group.	Yes	No	No
57002	warning	Survivable Remote Gateway	Survivable Remote Gateway - DN:XXX, Test Local Mode.	No Action Required.	Yes	No	No
57003	warning	Survivable Remote Gateway	Survivable Remote Gateway - DN:XXX, Local Mode – Firmware is out of sync with Main Office Call Server.	Check your firmware on the system to ensure it's the same revision as the main office.	Yes	No	No
57004	warning	Survivable Remote Gateway	Survivable Remote Gateway - DN:XXX, Local Mode – Set Firmware Upgrade in Progress.	No Action Required.	Yes	No	No

57005	warning	Survivable Remote Gateway	Survivable Remote Gateway - DN:XXX, Normal Mode – Set Redirected to Main Office.	No Action Required.	Yes	No	No
57006	warning	Survivable Remote Gateway	Survivable Remote Gateway - DN:XXX, Local Mode – Redirection Pending (Set on call).	No Action Required.	Yes	No	No
57007	warning	Survivable Remote Gateway	Survivable Remote Gateway - DN:XXX, Local Mode – Firmware Upgrade Pending (Set on call).	No Action Required.	Yes	No	No
57008	warning	Survivable Remote Gateway	Survivable Remote Gateway - DN:XXX, Local Mode – Main Office Parameters Not Provisioned.	Check your local configuration in the system.	Yes	No	No
57250	minor	Survivable Remote Gateway	Survivable Remote Gateway - DN:XXX, Invalid ID (1) – No endpoint in Gatekeeper database.	Check your configuration in the main office.	Yes	No	No

## 204 List of alarms

57251	minor	Survivable Remote Gateway	Survivable Remote Gateway - DN:XXX, Invalid ID (2) – ID unknown within the Call Server.	Check your configuration in the main office.	Yes	No	No
57252	minor	Survivable Remote Gateway	Survivable Remote Gateway - DN:XXX, Invalid ID (3) – Endpoint in Gatekeeper database is Originating Call Server.	Check your configuration in the main office.	Yes	No	No
57253	major	Survivable Remote Gateway	Survivable Remote Gateway - DN:XXX, Local Mode – Net Connect Server Unreachable.	Check your local configuration, network connectivity and ensure the main office is on line.	Yes	Yes	Yes
57500	major	Survivable Remote Gateway	Survivable Remote Gateway - DN:XXX, Local Mode – Main Office TPS Unreachable.	Check your local configuration, network connectivity and ensure the main office is on line.	Yes	Yes	Yes
57501	major	Survivable Remote Gateway	Survivable Remote Gateway - DN:XXX, Local Mode – Firmware is not available on the SRG.	Check your firmware on the system to ensure it's the same revision as the main office.	Yes	Yes	Yes

57750	critical	Survivable Remote Gateway	Survivable Remote Gateway - SRG terminated unexpectedly.	Contact your local support group.	Yes	Yes	Yes
60005	critical	LAN Driver	LAN Driver - Duplicate IP address detected on startup of LAN interface.	Check in diagnostics logs for messages log for further information. Also Check your network to ensure no other devices are using the same IP address as the system.	Yes	Yes	Yes
62009	warning	LAN Driver	Customer LAN is configured as a DHCP client but the address could not be obtained from the DHCP server.	Verify connectivity to the DHCP server or assign static address to the Customer LAN.	Yes	Yes	No
74200	major	NAT Dial-In	NAT Dial-In - NAT Kernel Loadable Module is not responding	No action required if a NAT Kernel Loadable Module patch has been applied or a system startup failure has occurred. Otherwise, contact your local support group.	Yes	Yes	Yes

206 List of alarms

74201	warning	NAT Dial-In	NAT Dial-In - "LAN side" addresses in the NAT configuration of all accounts do not fall in the customer LAN subnet on account <account>.	Ensure that the NAT mapping is updated accordingly. This may occur following either a system restore or a change in the customer LAN subnet where the customer LAN subnet conflicts with the NAT rules.	Yes	No	No
74202	warning	NAT Dial-In	NAT Dial-In - "Dial-In" address found in customer LAN subnet for account: <account>.	Ensure that the NAT mapping is updated accordingly. This may occur following either a system restore or a change in the customer LAN subnet where the customer LAN subnet conflicts with the NAT rules.	Yes	No	No

74203	minor	NAT Dial-In	NAT Dial-In - Error reading from account database for <account>	Retry the refresh on the screen or try again later. Alternatively, restart the BCM_NATProviderAgent Service. If the problem persists, restart the WANServiceMgr Service which will cause all dialup connections to be reset.	Yes	No	No
74204	minor	NAT Dial-In	NAT Dial-In - Error writing to account database <account>	Retry again later or reboot the BCM.	Yes	No	No
74205	minor	NAT Dial-In	NAT Dial-In - Error enabling NAT Rules for account <account> on <device>	Disconnect and retry the Dial-In connection.	Yes	No	No

## 208 List of alarms

---

74206	minor	NAT Dial-In	NAT Dial-In - Error disabling NAT Rules for account <account> on <device>	Restart the WANService-Mgr Service. As a side effect, all Dialup connections will be disconnected.	Yes	No	No
-------	-------	-------------	---	--	-----	----	----





## Nortel Business Communications Manager 450 1.0

# Fault and Performance Management

Copyright © 2008, Nortel Networks. The information in this document is sourced in Canada, the United States, India and the United Kingdom.

All Rights Reserved.

Publication: NN40160-701  
Document status: Standard  
Document issue: 01.01  
Document date: August 2008  
Product release: BCM450 1.0  
Job function: Fault and Performance  
Type: Technical Publication  
Language type: EN

NORTEL, the globemark design, and the NORTEL corporate logo are trademarks of Nortel Networks.  
Windows is a trademark of Microsoft Corporation.  
All other trademarks are the property of their respective owners.

To provide feedback or report a problem with this document, go to [www.nortel.com/documentfeedback](http://www.nortel.com/documentfeedback).

