Cisco BroadWorks

Network Server Fault and Alarm

Interface Specification

Document Revision History

Release	Version	Reason for Change	Date	Author
23.0	1	Created document	November, 2018	Gabriel Petrella
23.0	1	Updated content for Release 23.0.	November 15, 2018	Gabriel Petrella
23.0	1	Validated changes and published document.	December 3, 2018	Margot Hovey-Ritter
23.0	2	Completed rebranding for Cisco and republished document.	March 10, 2019	Margot Hovey-Ritter
2020.07_1.01	1	Updated content for 2020.07_1.01 build.	July 2, 2020	Charles Leduc
2020.07_1.01	1	Validated content and published document.	July 2, 2020	Margot Hovey-Ritter

Table of Contents

List of Figures

List of Tables

1 History of Changes to the Cisco BroadWorks Fault MIBs

This section provides the list of changes to the Cisco BroadWorks MIBs between releases.

1.1 Changes from Release 23.0 to Release 2020.07_1.010

This section provides the changes to Cisco BroadWorks MIBs between Release 2020.07_1.010 and Release 23.0, the previous major release of Cisco BroadWorks. Note that it also includes information related to service packs from the previous major release.

1.1.1 Added Faults

List of faults added for Release 2020.07_1.010.

Table 1: Added Faults for Release 2020.07_1.010

Fault Name	Mib	Feature	Also Available
bwOCICServerUnreachable	BroadworksFault.mib	PR-62549	None
bwOCIPServerUnreachable	BroadworksFault.mib	PR-62549	None
bwOSMisconfiguration	BroadworksFault.mib	PR-63831	None

1.1.2 Moved Faults

List of faults moved between MIBs for Release 2020.07_1.010.

No faults were moved in this release.

1.1.3 Deprecated or Obsoleted Faults

List of faults deprecated or obsoleted for Release 2020.07_1.010. Faults are either deprecated or obsoleted. The Status column indicates the status of the fault.

Table 2: Deprecated or Obsoleted Faults for Release 2020.07_1.010

Fault Name	Mib	Status
bwApplicationServerProvUnreachable	BroadworksFault.mib	Before: current After: obsolete

1.1.4 Removed Faults

List of faults removed for Release 2020.07_1.010.

No faults were removed in this release.

1.2 Changes from Release 22.0 to Release 23.0

This section provides the changes to Cisco BroadWorks MIBs between Release 23.0 and Release 22.0, the previous major release of Cisco BroadWorks. Note that it also includes information related to service packs from the previous major release.

1.2.1 Added Faults

List of faults added for Release 23.0.

Table 3: Added Faults for Release 23.0

Fault Name	Mib	Feature	Also Available
bwCentralizedDatabasePoolFailure	BroadworksFault.mib	PR-61058	None
bwNsCallPTimingVerificationQueryDegradation	BW-NSExecutionFault.mib	PR-59819	None

1.2.2 Moved Faults

List of faults moved between MIBs for Release 23.0.

No faults were moved in this release.

1.2.3 Deprecated or Obsoleted Faults

List of faults deprecated or obsoleted for Release 23.0. Faults are either deprecated or obsoleted. The Status column indicates the status of the fault.

Table 4: Deprecated or Obsoleted Faults for Release 23.0

Fault Name	Mib	Status
bwPMconfigdOutOfMemory	BroadworksConfigurationFault.mib	Before: current After: obsolete
bwPMlmdOutOfMemory	BW-LicenseManagerFault.mib	Before: current After: obsolete

1.2.4 Removed Faults

List of faults removed for Release 23.0.

Table 5: Removed Faults for Release 23.0

Fault Name	Mib
bwApplicationServerUnreachable	BroadworksFault.mib
bwNSCallPTimingVerificationQueryDegradation	BW-NSExecutionFault.mib

1.3 Changes from Release 21.0 to Release 22.0

This section provides the changes to Cisco BroadWorks MIBs between Release 22.0 and Release 21.0, the previous major release of Cisco BroadWorks. Note that it also includes information related to service packs from the previous major release.

1.3.1 Added Faults

List of faults added for Release 22.0.

Table 6: Added Faults for Release 22.0

Fault Name	Mib	Feature	Also Available
bwApplicationServerProvUnreachable	BroadworksFault.mib	PR-63437	None
bwCentralizedDatabaseListenerFailure	BroadworksFault.mib	PR-52073	None
bwCentralizedDatabaseMaxConnectionsReached	BroadworksFault.mib	PR-52342	None
bwCentralizedDatabaseNewConnectionFailure	BroadworksFault.mib	PR-52871	None
bwCouchbaseNodeConnectivityFailure	BroadworksFault.mib	*BW-10066*	R22.0

Fault Name	Mib	Feature	Also Available
bwExtremeOverload	BroadworksFault.mib	PR-45925	None
bwHazelcastClusterConnectivityUnavailable	BroadworksFault.mib	*BW-18485*	R22.0, R23.0
bwJVMProcessOutOfMemory	BroadworksFault.mib	*BW-6517*	R22.0
bwJVMProcessUnexpectedSoftwareCondition Detected	BroadworksFault.mib	*BW-6517*	R22.0
bwNetworkDatabaseClusterConnectivityFailure	BroadworksFault.mib	*BW-2299*	R21.sp2, R22.0
bwNetworkDatabaseNodeConnectivityFailure	BroadworksFault.mib	*BW-2299*	R21.sp2, R22.0
bwNetworkDatabaseSchemaFailure	BroadworksFault.mib	*BW-2299*	R21.sp2, R22.0
bwNSSyncSuccessDbCommitFailed	BroadworksFault.mib	BW-6957	None
bwProtocolRegistrationFailure	BroadworksFault.mib	PR-63437	None
bwPushNotificationServerUnreachable	BroadworksFault.mib	TIII-58132	None
bwTimeSkewExceeded	BroadworksFault.mib	*BW-2300*	R20.sp1, R21.sp1, R22.0
bwLocalXSBlacklisted	BW-NSExecutionFault.mib	*BW-11798*	R20.sp1, R22.0, R23.0
bwNSBlacklisted	BW-NSExecutionFault.mib	*BW-11798*	R20.sp1, R22.0, R23.0
bwNSCallPTimingVerificationQueryDegradation	BW-NSExecutionFault.mib	*BW-11798*	R20.sp1, R22.0, R23.0
bwNSCallPTimingVerificationThresholdExceeded	BW-NSExecutionFault.mib	*BW-11798*	R20.sp1, R22.0, R23.0
bwNSCallPTimingVerificationToolFailure	BW-NSExecutionFault.mib	*BW-11798*	R20.sp1, R22.0, R23.0
bwRemoteXSBlacklisted	BW-NSExecutionFault.mib	*BW-11798*	R20.sp1, R22.0, R23.0

1.3.2 Moved Faults

List of faults moved between MIBs for Release 22.0.

No faults were moved in this release.

1.3.3 Deprecated or Obsoleted Faults

List of faults deprecated or obsoleted for Release 22.0. Faults are either deprecated or obsoleted. The Status column indicates the status of the fault.

Table 7: Deprecated or Obsoleted Faults for Release 22.0

Fault Name	Mib	Status
bwNonheapMemoryUsageExceeded	BroadworksFault.mib	Before: current After: deprecated

1.3.4 Removed Faults

List of faults removed for Release 22.0.

No faults were removed in this release.

1.4 Changes from Release 20.0 to Release 21.0

This section provides the changes to Cisco BroadWorks MIBs between Release 21.0 and Release 20.0, the previous major release of Cisco BroadWorks. Note that it also includes information related to service packs from the previous major release.

1.4.1 Added Faults

List of faults added for Release 21.0.

Table 8: Added Faults for Release 21.0

Fault Name	Mib	Feature	Also Available
bwLocationServiceUnreachable	BroadworksFault.mib		
bwSystemBackwardTimeDrift	BroadworksFault.mib		
bwLicensingLMCommunicationLoss	BW-LicenseManagerFault.mib	*217550*	R20.sp1, R21.0
bwLicensingLMCommunicationLossGrace	BW-LicenseManagerFault.mib	*217550*	R20.sp1, R21.0
bwLicensingNFMCommunicationLoss	BW-LicenseManagerFault.mib	*217550*	R20.sp1, R21.0
bwLicensingNFMCommunicationLossGrace	BW-LicenseManagerFault.mib	*217550*	R20.sp1, R21.0
bwLicensingOverAllocation	BW-LicenseManagerFault.mib	*217550*	R20.sp1, R21.0
bwLicensingViolation	BW-LicenseManagerFault.mib	*217550*	R20.sp1, R21.0
bwLicensingViolationGrace	BW-LicenseManagerFault.mib	*217550*	R20.sp1, R21.0
bwOverAllocationViolationGrace	BW-LicenseManagerFault.mib	*217550*	R20.sp1, R21.0
bwPMlmdDeath	BW-LicenseManagerFault.mib	*217550*	R20.sp1, R21.0
bwPMlmdLaunched	BW-LicenseManagerFault.mib	*217550*	R20.sp1, R21.0
bwPMlmdOutOfMemory	BW-LicenseManagerFault.mib	*217550*	R20.sp1, R21.0
bwPMlmdRestarted	BW-LicenseManagerFault.mib	*217550*	R20.sp1, R21.0
bwPMlmdShutDown	BW-LicenseManagerFault.mib	*217550*	R20.sp1, R21.0
bwInterClusterConnectionFailure	BW-NSProvisioningFault.mib	*213706*	R21.0
bwSslClientAuthWithoutTrust	BW-WebContainerFault.mib	*173615*	R20.0

1.4.2 Moved Faults

List of faults moved between MIBs for Release 21.0.

No faults were moved in this release.

1.4.3 Deprecated or Obsoleted Faults

List of faults deprecated or obsoleted for Release 21.0. Faults are either deprecated or obsoleted. The Status column indicates the status of the fault.

No faults were deprecated or obsoleted in this release.

1.4.4 Removed Faults

List of faults removed for Release 21.0.

No faults were removed in this release.

2 Introduction

This document describes Cisco BroadWorks Fault Management for all the Cisco BroadWorks servers.

This document describes the:

- Cisco BroadWorks Fault Management components, including the Command Line Interface (CLI) and Simple Network Management Protocol (SNMP) functionality
- Notifications and alarms generated by Cisco BroadWorks

Cisco BroadWorks supports SNMP v2c and v3. Operators are provided with a set of comprehensive CLI commands to manage the SNMP trap redirection. Note that Cisco BroadWorks also acts as an SNMP proxy agent for the Solaris platform agent.

3 SNMP Agent Configuration

The information provided in this section applies to the SNMP agent for all the Cisco BroadWorks servers.

3.1 SNMP Agent Configuration

The Cisco BroadWorks SNMP interface is configured using the CLI client (bwcli). An operator has access to the SNMP configuration level at the CLI *Interfaces/SNMP* level.

```
CLI/Interface/SNMP> ?
    0)         AccessList : go to level AccessList
    1)              Agent : go to level Agent
    2)             AgentX : go to level AgentX
    3)  JVMStatsCollector : go to level JVMStatsCollector
    4)            Logging : go to level Logging
    5)            NetSNMP : go to level NetSNMP
    6)          Reporting : go to level Reporting
    7)               SMAP : go to level SMAP
    8)           TrapTable : go to level TrapTable
    9)    V3AccessControl : go to level V3AccessControl
   10)            V3Users : go to level V3Users

  h (help),  e (exit),  q (quit),  r (read),  w (write),  t (tree),
  c (config),  cd (cd),  a (alias),  hi (history),  p (pause),  re (repeat),
  k (keyboardHelp)


CLI/Interface/SNMP> Agent

CLI/Interface/SNMP/Agent> get
  port = 8001
  encoding = ISO-8859-1
  readCommunity = public
  writeCommunity = public
  trapCommunity = public
  trapSourceAddress = 192.168.13.189
  disableV2 = false
  hostMibII = false
```

By default, Cisco BroadWorks listens on port 8001 to service SNMP get requests. Compared to other typical SNMP agents, the Cisco BroadWorks agent cannot listen on port 161. Note that the community strings apply only for v2c requests.

For a system with multiple network interfaces, the operator can also choose the interface to use to send SNMP traps. In the example above, 192.168.13.189 appears as the trap source address received at the Element or Network Management System.

NOTE: At this context, the Logging context is used to configure logging and SMAP is used to configure internal messaging parameters. For information on the V3AccessControl and V3Users contexts, see the *BroadWorks Network Server Performance Measurement Interface Specification Guide*.

3.2 Configuration SNMP V2c Access List

An access list specifies the management systems permitted to retrieve performance measurements. The management system that sends the query must include, as part of the message, a community name that acts as a password on the agent systems. Upon each SNMP get request, Cisco BroadWorks verifies the

community and the IP address of the request against the community and IP address configured in the access list. Upon successful validation, the SNMP get request is processed. The access list is configured through the CLI.

```
CLI/Interface/SNMP> AccessList

CLI/Interface/SNMP/AccessList> get

   192.168.8.181
   192.168.8.179
       127.0.0.1
    192.168.8.43
  192.168.13.187
  192.168.13.185
   192.168.8.251

7 entries found.
```

3.3 SNMP Trap Managers

A trap-forwarding table specifies the management systems and the corresponding ports faults. The trap table is configured through the CLI.

```
AS_CLI/Interface/SNMP/TrapTable
AS_CLI/Interface/SNMP/TrapTable get
      IP Address  Port   Model  Use Alarms  V3User
================================================
   192.168.8.179  8001  shared        true
   192.168.8.181  8001  shared        true
    192.168.8.43  8001  shared        true
  192.168.13.187  8001  unique        true
  192.168.13.185  8001  unique        true
   192.168.8.251  8001  shared        true

6 entries found.
```

Cisco BroadWorks uses the concept of a model to control traps. The model value can either be set to "unique" or "shared". Details of these include:

- In the "unique" model, each Cisco BroadWorks trap has a unique OID. In this model, the management system does not have to do additional processing to uniquely identify a trap.

Important: Usage of the "unique" model is recommended.

- In the "shared" model, Cisco BroadWorks traps all use the same notification OID. Following this model, the management system must parse incoming traps and extract the fault name to uniquely identify each notification. The "shared" model was originally the only model supported by Cisco BroadWorks and it has been kept for backward-compatibility. It should only be used if a monitoring system still has scripts that use this functionality and that cannot be converted to use unique OIDs. As of Release 16.0, the "shared" model is deprecated. It is still fully supported; however, steps should be taken to convert monitoring managers relying on this model to the "unique" model.

3.4 SNMP v3 Access Control

SNMP agent configuration provides the ability to enforce the SNMP v3 View-based Access Control Model (VACM). This access control facility makes it possible to configure different levels of access to the agent Management Information Base (MIB) for SNMP v3 users. Access control is performed by a group, where

the group is a set of one or more users. Access is granted for each group to one of the three predefined views: *all*, *management*, or *performance*.

- The *all* view provides access to all MIBs.
- The *management* view provides access to the managed object's subtree from the Cisco BroadWorks maintenance MIB (*BroadworksMaintenance.mib*).
- The *performance* view provides access to all other MIBs. Read and write permissions are given on a per-user basis.

The following figure illustrates the three predefined views.

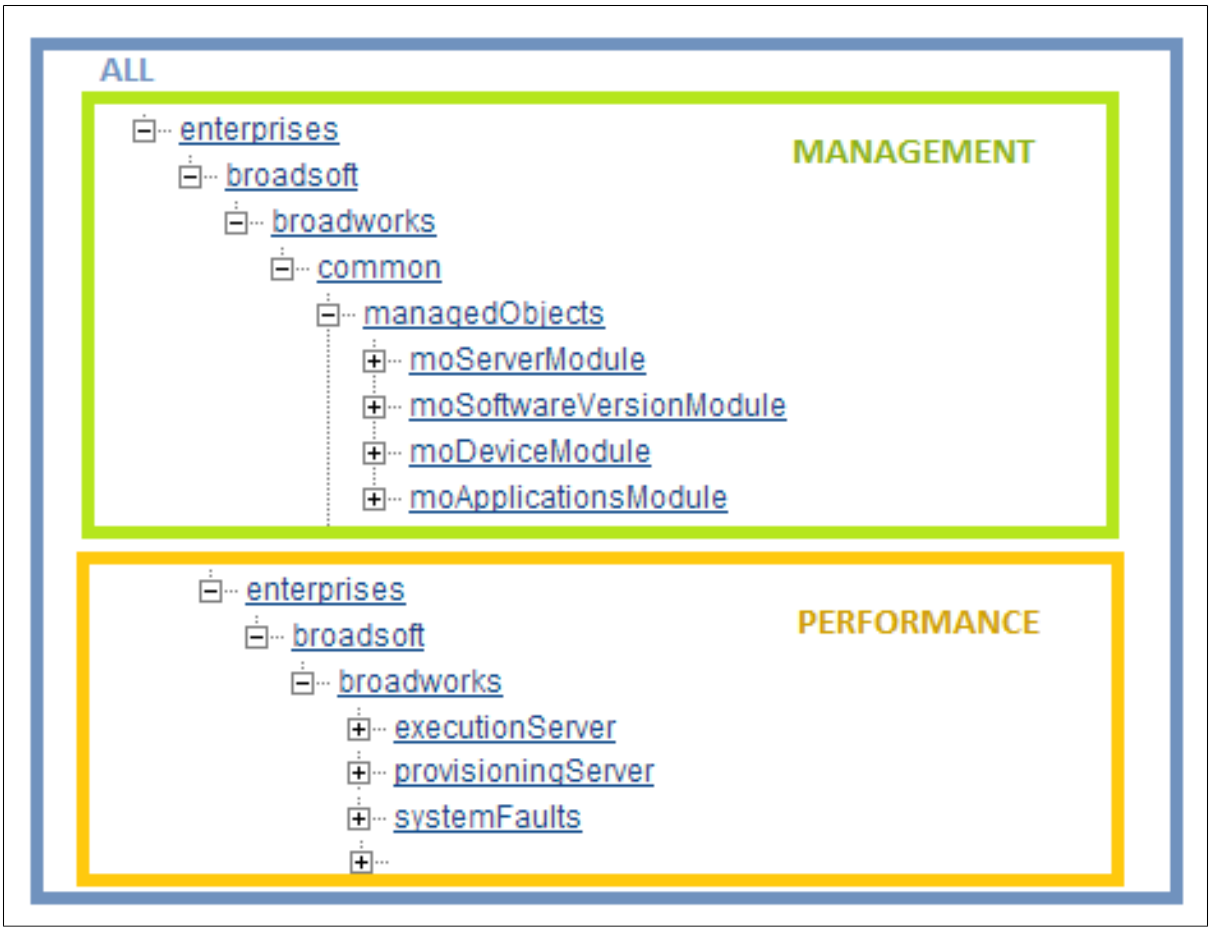

Figure 1: Views

Both the VACM and the User-based Security Model (USM) MIBs are solely allowed "read-only" access. Configuration of the settings for v3 access control is performed through the Cisco BroadWorks CLI.

First, define an access control group and then set the level of access for the group. More than one level of access can be assigned to a group. The following illustrates these steps from the CLI.

```
CLI/Interface/SNMP/V3AccessControl/Groups> add groupOne
...Done

CLI/Interface/SNMP/V3AccessControl/Groups> get
      Name
==========
  groupOne

1 entry found.
```

```
CLI/Interface/SNMP/V3AccessControl/Groups> AccessLevels
CLI/Interface/SNMP/V3AccessControl/Groups/AccessLevels> add groupOne performance
...Done

CLI/Interface/SNMP/V3AccessControl/Groups/AccessLevels> get groupOne
       Level
============
 performance

1 entry found.
```

3.5 SNMP v3 Users

SNMP v3 uses a User-based Security Model (USM). Management operations using this security model make use of a defined set of user identities. For any user with management operations authorized at a particular SNMP engine, that SNMP engine must have knowledge of that user. An SNMP engine that wishes to communicate with another SNMP engine must also have knowledge of a user known to that engine, including knowledge of the applicable attributes of that user.

The Cisco BroadWorks v3 implementation supports three levels of v3 users:

- No Authorization, No Privacy
- Authorization (MD5, SHA, SHA224, SHA256, SHA384, SHA512), No Privacy
- Authorization (MD5, SHA, SHA224, SHA256, SHA384, SHA512), Privacy (DES, AES)

A v3 user can be associated with an access control group. Configuration of the SNMP v3 users is done through the Cisco BroadWorks CLI.

NOTE: If no access control group is assigned to a v3 user, that user has no access.

3.6 Reporting

The SNMP reporting level allows an operator to automate the generation of an operational measurements report, which is sent to remote servers. The report (in XML format) contains a header and a value for each SNMP counter and gauge. The report is sent to remote servers via FTP put commands.

For more information on reporting functionality, see the *BroadWorks Network Server Performance Measurement Interface Specification Guide*.

4 Cisco BroadWorks Faults

This section provides the definitions required to work with the Cisco BroadWorks faults.

4.1 Fault Template

The following table describes the fields in a fault report:

Table 9: Fault Report Fields

Field	Description
Identifier	A sequentially generated number, which can be used to uniquely identify the fault.
Timestamp	The date and time the fault was generated.
System Name	The host name of the system running Cisco BroadWorks software.
Severity	An indicator of the severity of the fault. **INFORMATIONAL:** This does not affect service. **LOW:** Losing redundant connectivity, but does not affect service or capacity. For example, the primary SMTP server is down, but Call Notify services are still provided via secondary SMTP server (for example, losing one Media Server). (The Media Server is typically deployed in N + 1 fashion). **MEDIUM:**Ability to provide connectivity, but affects service-level. For example, losing two out of four Media Servers impacts the Media Server capacity. **HIGH:** Inability to provide connectivity over a particular interface. For example losing connectivity to all Media Servers or losing connectivity to both SMTP servers. **CRITICAL:** No basic calls can be processed without operator intervention.
Component	The Cisco BroadWorks server or application reporting the fault.
Subcomponent	Software component within the Cisco BroadWorks component reporting the fault.
Problem Type	Notification, Alarm, or Software Error
Alarm State	Alarm "On" or "Off" (applicable to stateful alarms only).
Problem Text	Text indicating the details of the variable. One central file for problem text to support internationalization.
Problem Resources	A list of variables, which bind to the problem text.
Recommended Actions Text	Text indicating details of the recommended actions to take.
Recommended Resources Text	A list of variables, which bind with the recommended actions text.
Notification Parameters variable bindings...	Each fault defines a number of variable bindings that give additional context to the fault being sent.

The remaining sections specify faults generated by Cisco BroadWorks. The document is organized by component followed by subcomponent. Variable bindings for Problem Text parameters are denoted by *%<tagName>%*, where <tagname> is the name of the notification parameter that is itself featured as a variable binding in the SNMP trap. Variable bindings for *Recommendation Text* parameters are denoted by *%n*, where n is an integer representing the argument number. Carriage returns in the *Problem Text* and *Recommendation Text* fields are denoted by <*cr*>.

4.2 Notifications and Alarms

Cisco BroadWorks defines two types of faults: notifications and alarms. Notifications describe punctual events that can occur throughout the lifetime of the application. Events such as unauthorized access,

security violations, status reports, added/deleted resources, unreachable servers, and software errors can be the objects of notifications. The system health report is a good example of a notification. A monitored device sends it periodically to provide a snapshot of its health at a certain moment. The severity of this notification depends on the health of the monitored device.

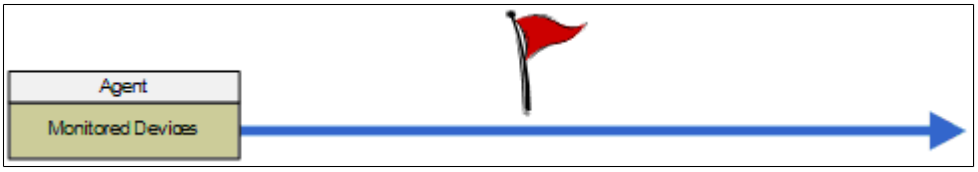

Figure 2: Visual Representation of Notification during Lifetime of Monitored Device

Alarms warn that the system is currently in an abnormal state, but that the situation could change (for better or worse) over time. Alarms are raised at the start of the abnormal state and are cleared upon return to normal state. They are used to represent events such as connectivity loss, unresponsive software components, reached threshold limits, and resource exhaustion. Alarms have a state that determines whether they are *On* or *Off*. Alarms are sometimes referred to as Stateful Alarms. An additional state, Cleared, is used when the alarm is set to *Off* through manual intervention. *Off* and Cleared mean the same thing except that the latter gives an indication that the alarm was set to *Off* manually.

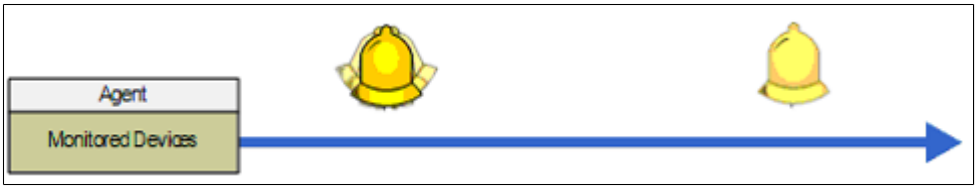

Figure 3: Visual Representation of Alarm during Lifetime of Monitored Device

4.3 Alarm Correlation

This feature introduces the correlation parameter. Monitoring systems can correlate with the alarm name to identify different instances of the same alarm when raised numerous times for different reasons.

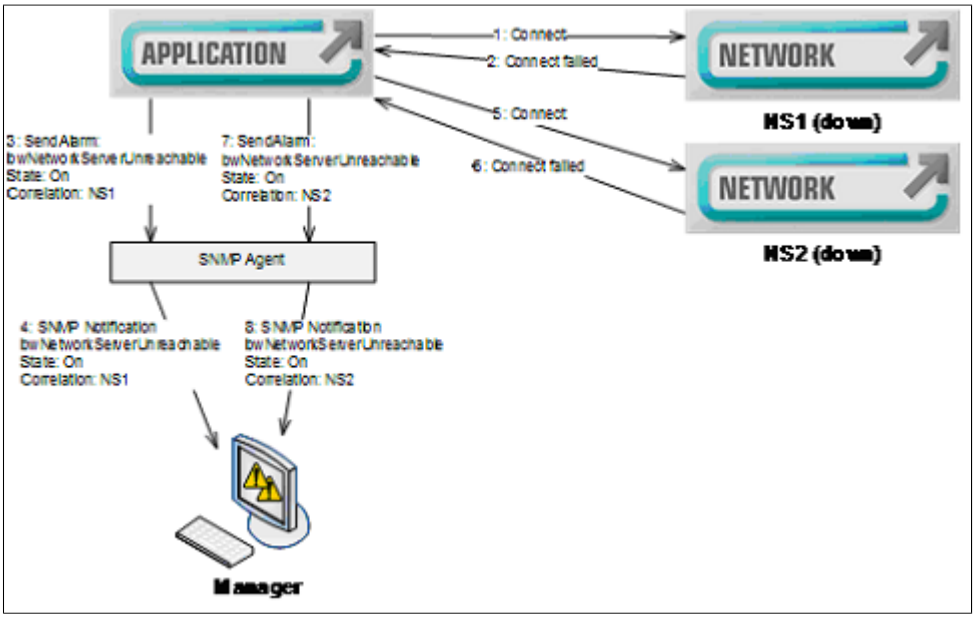

Figure 4: Visual Representation of Multiple Instances of Same Alarm being Raised

In **Figure 3** the Application Server tries to connect to two Network Servers; however, it fails. When an Application Server is unable to connect to a Network Server, the *bwNetworkServerUnreachable* alarm is raised. To differentiate between the alarms concerning NS1 and NS2, the monitoring system can now read the correlation variable which, in addition to the alarm name, correlates and uniquely identifies the alarm instance.

When the Application Server is finally able to connect to NS1, it sends a new alarm - *state* = "off" with the same differentiator variable. This way, the monitoring system knows which *bwNetworkServerUnreachable* alarm instance to clear.

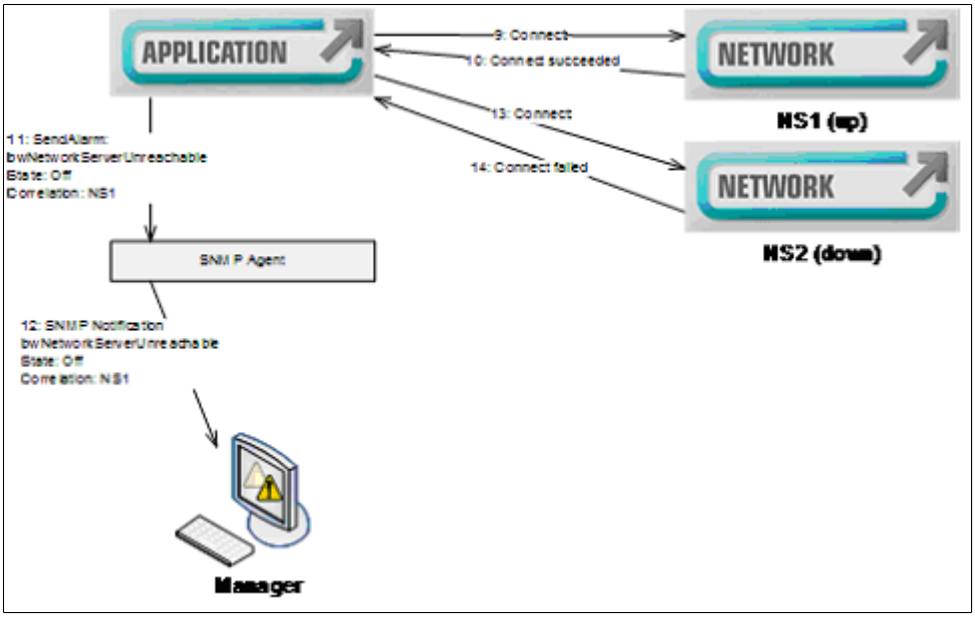

Figure 5: Visual Representation of Alarm Instance being Set to Off

The *correlation* parameter type is a string. This allows it to be generic enough for all alarm types that use it. For example, in the case of a connectivity problem, the correlation value could be the configured address; for software failures, the correlation value could be the component name, and so on.

The correlation parameter is defined at the following object identifier (OID):

```
.iso.org.dod.internet.private.enterprises.broadsoft.broadworks.
common.systemFaults.faultFields.correlationParameter
OID: .1.3.6.1.4.1.6431.1.1.1.1.11
```

NOTE: Monitoring managers shall always correlate alarms using the alarm OID and the correlation parameter.

4.3.1 Example

The *bwCNAMSoapServerUnreachable* notification is sent when an Application Server detects a connectivity problem with a CNAM (CNAM) SOAP server. In this example, the originating component is the Application Server and the subcomponent is the SOAP interface. The *BroadworksFault.mib* file defines the Application Server as component 0 and the SOAP interface as the subcomponent 47. In this example the unreachable CNAM SOAP server is at address *192.168.8.13* and the exception message is *unknown*.

The correlation parameter for this alarm would be a composition of the component, the subcomponent, and all the problem variables:

```
0;47;192.168.8.13;unknown
```

The same correlation parameter is calculated when the alarm state is set to *Off*, allowing managers to clear the alarm.

4.3.2 High Availability SNMP Alarms

One of the SNMP agent challenges is to provide high availability for SNMP alarms even though they are transferred over the unreliable User Datagram Protocol (UDP). High availability is achieved by providing access to active and historical alarms as well as re-sending alarms following an agent failure.

4.3.2.1 List of Alarms

The agent sends SNMP alarms (traps/notifications) to the monitoring systems over the UDP protocol, a connectionless and unreliable protocol. It is possible that monitoring systems do not receive alarms at all. For this reason and because the monitoring systems can be restarted, the agent provides a list of currently active alarms. The agent maintains this table with the information coming from the subcomponents on the server.

```
The alarm list is located in the common maintenance MIB:
.iso.org.dod.internet.private.enterprises.broadsoft.broadworks.
common.alarms.bwAlarmsTableOID:
.1.3.6.1.4.1.6431.1.1.2.1
```

Managers can request alarms to be resent to them. Additionally, it is possible to clear currently active alarms.

The table contains up to a maximum of 500 (configurable through a Java property) alarms that are currently raised. The table displays the following alarms fields. All fields are read-only.

- *Sequential Identifier* (Counter32) - INDEX
- *Timestamp* (DateAndTime)
- *Alarm OID* (OID)
- *Alarm Name* (DisplayString)
- *Severity* (Integer: Informational (0), low (1), medium (2), high (3), critical (4))
- *Correlation Parameter* (DisplayString)

Two additional read-write fields are provided to perform actions on selected alarms:

- *Clear Alarm* (Integer: Clear (1))
- *Resend* (String)

The Sequential Identifier integer always counts up for each new notification and alarm. It is, therefore, not a sequential table row count.

In the event that the table limit is reached, no new alarms are generated by the agent. A critical notification, *bwAlarmsTableLimitReached*, is sent to notify monitoring managers that the agent is no longer processing alarms normally.

When the alarm state is set to *Off*, the originating component is notified that it must clear its alarm. This results in a new notification being sent to clear the alarm by the originating component.

The *Resend* field must be set with a valid host and port (format: host:port) for an alarm to be resent. Any valid combination of host and port can be used, as long as it is a configured manager and it is configured to support alarms. When set, the corresponding alarm is resent to the monitoring manager defined by the host and port. All original parameters are kept, including the timestamp. Note that it is possible that the resending of the alarms reaches the host after a possible clearing of the alarm. The monitoring manager must handle this scenario by comparing the timestamps and correlation parameters.

At the CLI, the list can also be consulted using the list command at the AlarmsTable level:

```
$ CLI/Monitoring/Alarms/AlarmsTable> list
Identifier   TimeStamp              Alarm Name                      Severity
 Correlation Parameter
=============================================================
```

```
2562          2010-3-23 20:48:50 GMT  bwNSSynchUnknownHostnameError    Medium
 2;16;MTLSOL-27;
1 entry found.
```

4.3.2.2 Component Failure

A component failure is defined as a component losing its communication with the SNMP agent while the SNMP agent itself is still alive. Loss of communication is detected by the Cisco BroadWorks Common Communication Transport (BCCT) framework which actively monitors the connection between the agent and SNMP agent for disconnections and socket failures. When the communication is re-established with the SNMP agent through a communication reset or through a restart of the component's process, the failure is resolved.

When a component failure is detected by the agent, it removes the outstanding alarms sent by this component from the alarms tables, and sends clearing notifications to the monitoring managers.

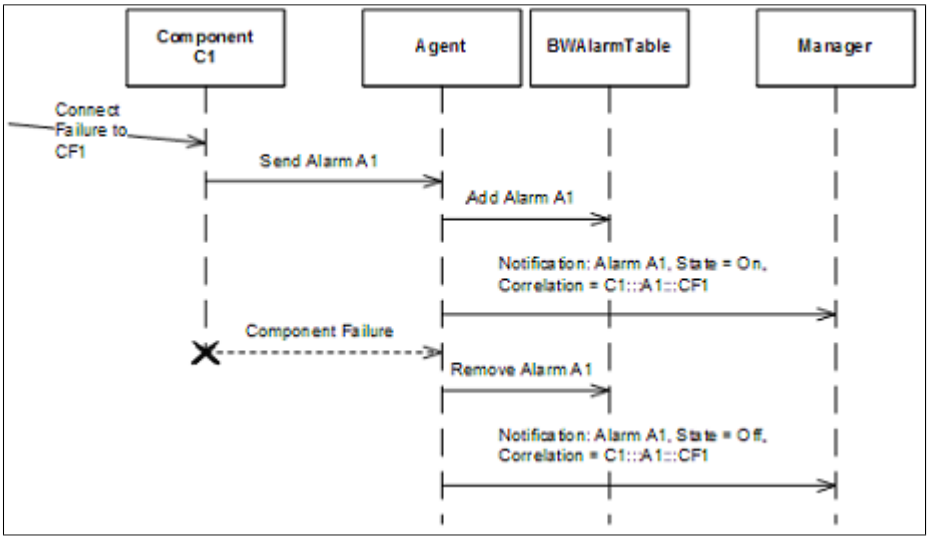

Figure 6: Component Failure

Upon resolution of the component failure, the component communicates active alarms to the agent who in turn sends them out to the managers.

Managers can check this table periodically to ensure they are synchronized and that they have not missed any alarms.

4.3.2.3 Agent Failure

In the event that the agent fails, it is automatically restarted by the process monitor. Although this situation is not supposed to occur, a strategy is in place to reduce the failure time while ensuring high availability of the alarm.

At startup or following a failure, the agent starts with an empty Alarms table. Upon reconnection of the different server's components with the SNMP agent, the table is repopulated with currently active alarms. Alarm raises or clears that occurred on the component during the agent failure are also sent to the agent who in turn sends out alarms to the managers.

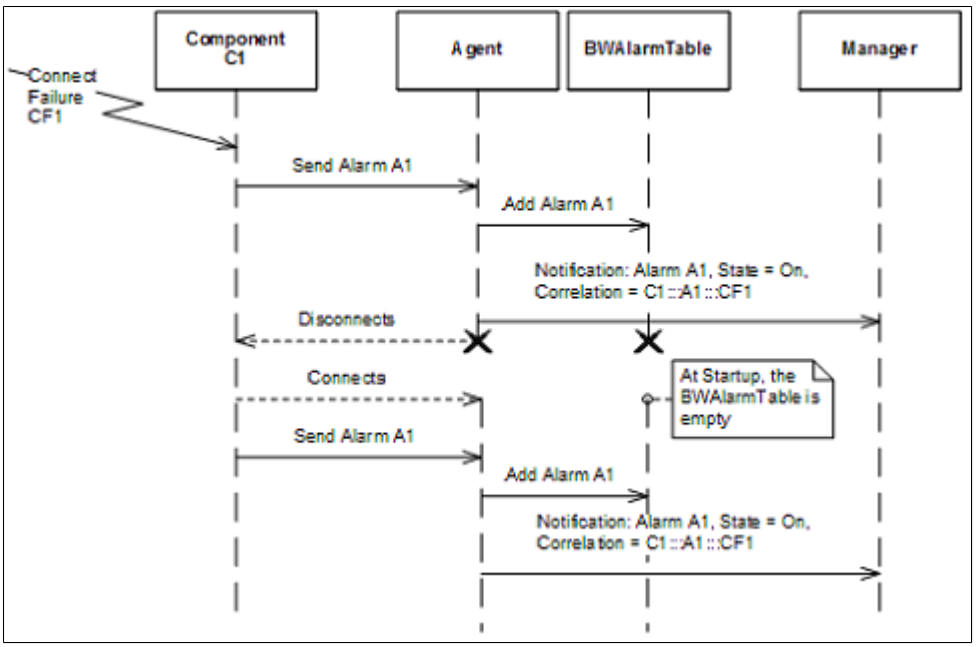

Figure 7: Agent Failure

In this scenario, if the manager did not detect the agent failure through a ping, it receives the same notification twice. In this case, the manager should update the initial alarm, which is identifiable with the correlation parameter. Note that if the component sends a notification indicating that it was just restarted, the manager could trigger on this notification to clear all the other alarms for this component.

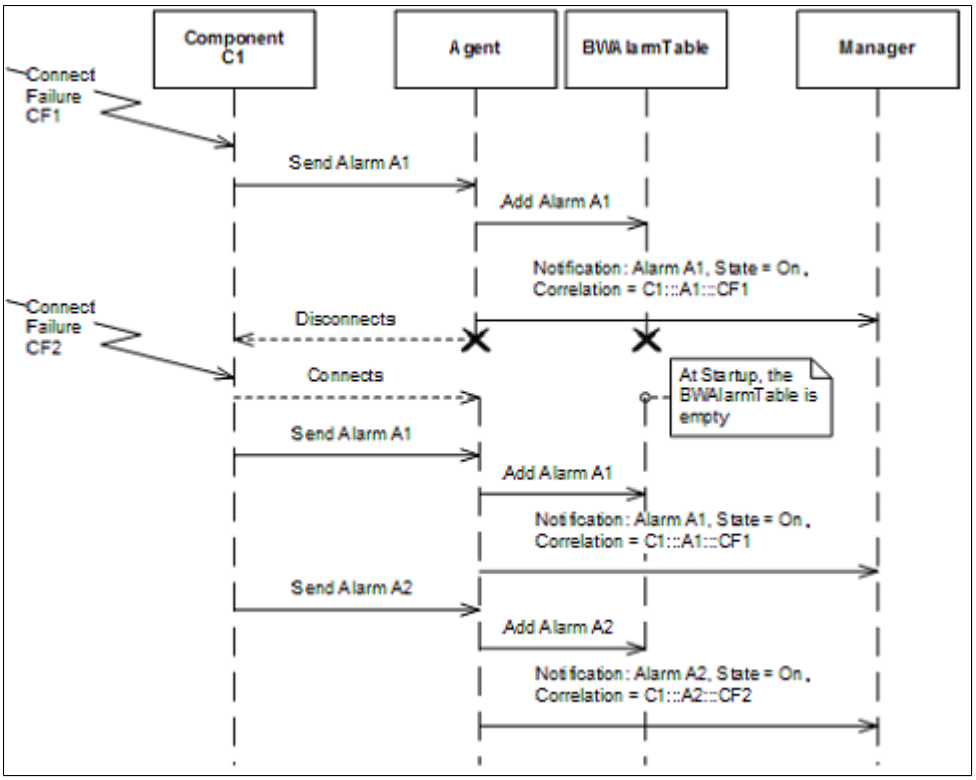

Figure 8: Agent Failure with Component Queuing Mechanism

In the case that a component detects an event noteworthy of an alarm while not connected to the SNMP agent, it queues the alarm until the connection is re-established.

4.3.2.4 Cisco BroadWorks Restart

When it starts, a notification is not sent by the agent. Even if there was one, their unreliable nature would not guarantee that all monitoring managers would receive it. Following a Cisco BroadWorks server restart, when problems are encountered, the agent generates new notifications. If they share the same correlation parameter, they might look like updates of past notifications to the monitoring managers.

Monitoring managers should perform periodic lookups (for example, 15 minutes) to ensure they remain synchronized.

4.3.2.5 Clear Alarm

Managers can clear any alarm in the Alarms table. To clear a specific alarm, the value of the corresponding alarm *clearAlarm* column must be set to *1*. When the agent receives such a request, it notifies the originating component. The originating component is responsible to send back, asynchronously, a message to the agent indicating that the alarm was cleared. The agent then sends an alarm clear to all monitoring managers. When an alarm is manually cleared, its state should be *Cleared*.

It is also possible to clear an alarm using the CLI:

```
$ CLI/Monitoring/Alarms/AlarmsTable> clear 134
...Done
```

NOTE: Because the agent must request the clear to another component, there is absolutely no guarantee that a request to clear an alarm results in a *Cleared* notification to be issued.

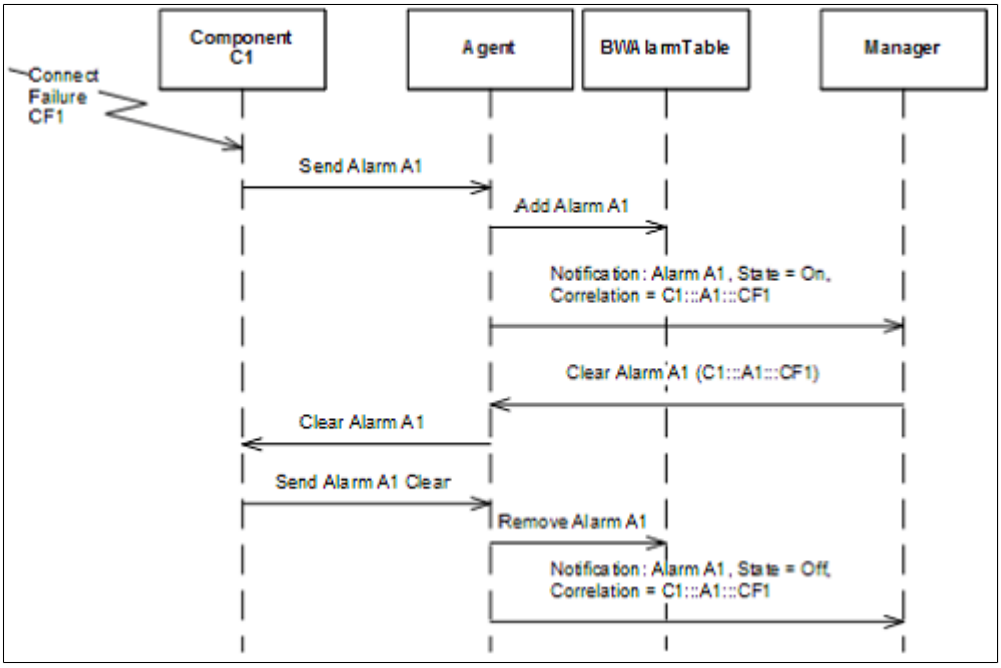

Figure 9: Clearing Alarm from Manager

4.3.2.6 Clearing the Alarms

It is possible to clear the alarm list from the agent through a unique SNMP operation. This has the same effect as clearing every single alarm individually.

The entire alarm list can be reset by setting the integer value 1 on the following OID:

```
.iso.org.dod.internet.private.enterprises.broadsoft.broadworks.
common.alarms.resetAlarmsTable
OID: .1.3.6.1.4.1.6431.1.1.4.2
```

The clearing of the Alarms table can also provisioned at the CLI:

```
$ CLI/Monitoring/Alarms/AlarmsTable> clearAll
WARNING: This will clear all currently active alarms. Every configured manager will
 receive many notifications.
Please confirm (Yes, Y, No, N): y
...Done
```

NOTE: Resetting the entire alarm list might trigger as many notifications as there are active alarms. To prevent the flooding of the monitoring managers, this operation is by default permitted only once every 30 seconds (configurable through the *resendAllRequestPeriod* property) for all monitoring managers.

4.3.2.7 Resending All Alarms in Alarms Table

In the event that a monitoring manager requires SNMP notifications to be sent to re-synchronize due to an impossibility of synchronization based on the information contained in the Alarms table, it is possible to have all the current alarms resent.

```
The entire alarm list can be resent through SNMP notifications by setting the address
 and the port of a configured monitoring manager that uses alarms (format:  host:port)
 on the following OID:
.iso.org.dod.internet.private.enterprises.broadsoft.broadworks.
common.alarms.resendAlarmsTableOID:
.1.3.6.1.4.1.6431.1.1.4.3
```

Resending all alarms in the Alarms table can also be done at the CLI:

```
$ CLI/Monitoring/Alarms> resendAll 192.168.1.14 20001
        ...Done
```

NOTE: Resending all alarms of the Alarms table triggers as many notifications as there are active alarms. To prevent the flooding of the target monitoring manager, this operation is by default permitted only once every 30 seconds (configurable through the *clearAllRequestPeriod* property) per monitoring manager.

4.3.2.8 Last Modification Timestamp

Every time the Alarms table is modified, the agent updates a timestamp indicating the time at which the last modification to the table was made. This timestamp is exposed and can be used by monitoring managers in their effort to synchronize the table. Every time a monitoring manager wants to synchronize, it should compare its copy of the last modification timestamp with the one on the server before traversing the Alarms table. The timestamp is always set when the Cisco BroadWorks SNMP agent restarts, whether or not there are alarms in the table.

```
Node Name:
.iso.org.dod.internet.private.enterprises.broadsoft.broadworks.
common.alarms.lastAlarmsTableModificationTimestampOID:
.1.3.6.1.4.1.6431.1.1.4.4
```

4.3.2.9 Polling

The agent does not notify monitoring systems when it suddenly dies. Monitoring systems should poll the agent on a regular basis to ensure that it is still alive and that alarms reported earlier are still valid.

4.3.3 Notifications Parameterization

A weakness of the former SNMP agent implementation is the lack of contextualized parameters in notifications. All notifications are sent with the same parameters and one has to read the *Problem Text* field to understand what the root cause of the problem is.

This verbose behavior is acceptable for human beings who read complex sentences. However, it makes information systems parse the *Problem Tex*t field to gather the information it requires to deal with the alarm.

Notification parameters solve this problem. In addition to existing generic parameters, new contextualized parameters are added to notifications. For example, for connectivity problems, a new parameter *npRemoteAddress* is added. Notifications can have as many parameters as required to provide adequate context to network managers. Each fault definition in the MIBs defines the parameters they carry.

The following example shows how the *bwExternalAuthenticationUnknownUser* carries the *npUserName* and *npDomain* parameters when it is sent.

```
bwExternalAuthenticationUnknownUser  NOTIFICATION-TYPE
  OBJECTS { identifier, timestamp, alarmName, systemName, severity, component,
 subcomponent, problemText, recommendedActionsText, npUserName, npDomain}
  STATUS current
  DESCRIPTION
      "..."
  ::=  {  systemFaults 3583  }
```

5 External Subagents Integration

This section provides a list of SNMP subagents for which Cisco BroadWorks acts as proxy.

5.1 High-level Description

The integration of the SNMP subagents is performed through a master/proxy agent with subagent architecture.

The Cisco BroadWorks agent acts as a master/proxy agent to the other subagent(s) and provides a single point of access for managers. The master/proxy agent functionalities are as follows:

- Receives requests from managers
- Forwards requests to appropriate subagent
- Receives responses from subagent
- Forwards responses to managers
- Forwards traps to managers

The Cisco BroadWorks master SNMP agent listens for traps on port 162, thereby allowing any agent that is sending traps to port 162 to be captured by the master agent and forwarded to the appropriate managers. This is the case with the TimesTen application, which forwards traps to port 162 even though it is not defined as a subagent for the Network Server (NS) and the Application Server (AS). Note that TimesTen is not part of the Media Server (MS).

The authorization list for manager(s) accessing the system is managed through the existing Cisco BroadWorks SNMP agent access control list.

This feature is designed for network and system operators to monitor hardware and software devices on which Cisco BroadWorks applications are running and is available for Cisco BroadWorks servers.

5.2 Integrated Third-Party Subagents

Cisco BroadWorks integrates the following subagents:

- Solaris MIB II subagent
- TimesTen subagent (alarms only)

6 Fault Thresholding and Suppression

Fault suppression and threshold can be viewed as fault filters. This feature provides fault filtering at the Cisco BroadWorks SNMP agent level. The Cisco BroadWorks servers continue to generate faults. They send the faults to their SNMP agent (using a proprietary protocol) and the agent processes them. When the SNMP agent receives a fault, it performs the following tasks:

1) Logs the fault to a local file.
2) Sends the fault to a trap server, which then sends it to all registered trap clients (such as Cisco BroadWorks CLI sessions).
3) Sends an SNMP trap to the provisioned managers.

This feature only performs fault filtering for tasks one (1) and three (3) above. Therefore, fault filtering has no impact on trap clients waiting for faults.

The feature only provides a mechanism to filter faults generated by Cisco BroadWorks applications (such as the Application Server Execution Server, Application Server Provisioning Server, Network Server Execution Server, Network Server Provisioning Server, and so on) and Cisco BroadWorks process monitors. In other words, this feature provides filtering for faults defined under the Cisco Object Identifier (OID).

Fault filtering occurs at the SNMP agent-level (not by cluster).

6.1 Trap Lists

Currently, each Cisco BroadWorks server comes with XML-encoded trap list files which define all the traps that this server can generate. These files are:

Table 10: Traplist Files

Cisco BroadWorks Server	Traplist File Name
Common to all servers	*/usr/local/broadworks/bw_base/conf/commontraplist.xml /usr/local/broadworks/bw_base/conf/configdtraplist.xml*
Access Mediation Server	
Application Server	*/usr/local/broadworks/bw_base/conf/executiontraplist.xml /usr/local/broadworks/bw_base/conf/ocstraplist.xml /usr/local/broadworks/bw_base/conf/provisioningtraplist.xml /usr/local/broadworks/bw_base/web/conf/containertraplist.xml*
Call Detail Server	*/usr/local/broadworks/bw_base/conf/cdstraplist.xml /usr/local/broadworks/bw_base/conf/webcontainertraplist.xml*
Element Management System	*/usr/local/broadworks/bw_base/conf/emstraplist.xml /usr/local/broadworks/bw_base/conf/ocstraplist.xml /usr/local/broadworks/bw_base/web/conf/containertraplist.xml* Profile Server */usr/local/broadworks/bw_base/conf/pstraplist.xml /usr/local/broadworks/bw_base/confwebcontainertraplist.xml*
Media Server	*/usr/local/broadworks/bw_base/conf/mstraplist.xml*
Network Server	*/usr/local/broadworks/bw_base/conf/nsexecutiontraplist.xml /usr/local/broadworks/bw_base/conf/nsportaltraplist.xml /usr/local/broadworks/bw_base/conf/nsprovisioningtraplist.xml /usr/local/broadworks/bw_base/conf/webcontainertraplist.xml*
Profile Server	*/usr/local/broadworks/bw_base/conf/pstraplist.xml /usr/local/broadworks/bw_base/confwebcontainertraplist.xml*
Xtended Services Platform	*/usr/local/broadworks/bw_base/conf/xsptraplist.xml /usr/local/broadworks/bw_base/conf/ocstraplist.xml /usr/local/broadworks/bw_base/conf/webcontainertraplist.xml /usr/local/broadworks/bw_base/conf/uconnecttraplist.xml* (**NOTE**: This file appears once the application is activated.)

Although trap definitions are in every component's fault MIBs, some information is also defined in the trap list file. The trap list file hosts the problem text and recommended action text for all traps originating from a

Cisco BroadWorks component. This text is defined in a separate file to allow internationalization of these fields if required.

Traplist entry example:

```
   <trap>
      <name>bwTrunkGroupCapacityExceeded</name>
      <problemType>0</problemType>
      <problemText>The capacity of a trunk group was exceeded.
Service Provider / Enterprise Name: %npServiceProviderId%
Group Name: %npGroupName%
Trunk Group Name: %npTrunkGroupName%</problemText>
      <recommendedAction>Increase the Maximum Active Calls Allowed parameter of the
 associated trunk group.
Maximum Active Calls Allowed: *
Maximum Outgoing Active Calls Allowed: *
Maximum Incoming Active Calls Allowed: *
Bursting Maximum Active Calls Allowed *
Bursting Maximum Outgoing Active Calls Allowed: *
Bursting Maximum Incoming Active Calls Allowed: *
        <recommendedActionParam doc="Maximum Active Calls Allowed parameter" />
        <recommendedActionParam doc="Maximum Outgoing Active Calls Allowed parameter" /
>
        <recommendedActionParam doc="Maximum Incoming Active Calls Allowed parameter" /
>
        <recommendedActionParam doc="Bursting Maximum Active Calls Allowed parameter" /
>
        <recommendedActionParam doc="Bursting Maximum Outgoing Active Calls Allowed
 parameter" />
        <recommendedActionParam doc="Bursting Maximum Incoming Active Calls Allowed
 parameter" />
      </recommendedAction>
   </trap>
```

Variables in the problem text must be valid notification parameters described in the *BroadworksFault.mib* file. Conversely, the wildcard character for the recommended action text is always the asterisk (*). If this file must be internationalized, only the *problemText* and *recommendedAction* must be translated. The *recommendedActionParam* is for internal use and does not appear in the trap sent to the monitoring managers. When internationalizing, the problem text variables (between percent (%) signs) should not be modified.

6.2 Trap Filters

Trap filter files are XML-based files. The purpose of this file is different from the trap lists. Rather than defining trap information, they define fault filters that can be used to throttle or suppress faults sent by the SNMP agent.

Trap filters are defined in the following files:

Table 11: Trap Filter Files

BroadWorks Server	Trap Filter File Name
Access Mediation Server	
Application Server	*/usr/local/broadworks/bw_base/conf/astrapfilter.xml /usr/local/broadworks/bw_base/conf/ ocstrapfilter.xml*
Call Detail Server	*/usr/local/broadworks/bw_base/conf/cdstrapfilter.xml*
Element Management System	*/usr/local/broadworks/bw_base/conf/emstrapfilter.xml /usr/local/broadworks/bw_base/conf/ ocstrapfilter.xml*
Media Server	*/usr/local/broadworks/bw_base/conf/mstrapfilter.xml*

BroadWorks Server	Trap Filter File Name
Network Server	*/usr/local/broadworks/bw_base/conf/nstrapfilter.xml*
Profile Server	*/usr/local/broadworks/bw_base/conf/pstrapfilter.xml /usr/local/broadworks/bw_base/conf/ocstrapfilter.xml*
Xtended Services Platform	*/usr/local/broadworks/bw_base/conf/xsptrapfilter.xml /usr/local/broadworks/bw_base/conf/ocstrapfilter.xml*

The trap filter files are preserved during a BroadWorks upgrade so that filters defined by customers can remain unchanged after an upgrade.

Details on the Document Type Definition (DTD) for trap filter files follow.

```
<?xml version='1.0' encoding="UTF-8"?>

<!ELEMENT trapFilter    (defaultFilter?, filter*)>

<!ELEMENT defaultFilter    (active, maxNumTrapsPerTimePeriod, timePeriodInSeconds?,
 minSeverity?)>

<!ELEMENT filter    (name, active, maxNumTrapsPerTimePeriod, timePeriodInSeconds?,
 problemTextVarNum1?, problemTextVarNum2?, problemTextVarNum3?, problemTextVarNum4?,
 problemTextVarNum5?)>

<!ELEMENT name (#PCDATA)>
<!ELEMENT active (false|true)>
<!ELEMENT maxNumTrapsPerTimePeriod (#PCDATA)>
<!ELEMENT timePeriodInSeconds (#PCDATA)>
<!ELEMENT minSeverity (0|1|2|3|4)>
<!ELEMENT problemTextVarNum1 (#PCDATA)>
<!ELEMENT problemTextVarNum2 (#PCDATA)>
<!ELEMENT problemTextVarNum3 (#PCDATA)>
<!ELEMENT problemTextVarNum4 (#PCDATA)>
<!ELEMENT problemTextVarNum5 (#PCDATA)>

>
```

Assuming that astrapfilter.xml contains the following trapFilter block:

```
  <trapFilter>
    <defaultFilter>
      <active>false</active>
      <maxNumTrapsPerTimePeriod>10</maxNumTrapsPerTimePeriod>
      <timePeriodInSeconds>5</timePeriodInSeconds>
      <minSeverity>1</minSeverity>
    </defaultFilter>
    <filter>
      <name>bwSipRegistrationFailure</name>
      <active>true</active>
      <maxNumTrapsPerTimePeriod>0</maxNumTrapsPerTimePeriod>
    </filter>
    <filter>
      <name>bwSipUnexpectedMessage</name>
      <active>true</active>
      <maxNumTrapsPerTimePeriod>2</maxNumTrapsPerTimePeriod>
      <timePeriodInSeconds>5</timePeriodInSeconds>
    </filter>
    <filter>
      <name>bwNSSynchronizationFailure</name>
      <active>true</active>
      <maxNumTrapsPerTimePeriod>1</maxNumTrapsPerTimePeriod>
      <timePeriodInSeconds>10</timePeriodInSeconds>
```

```
      <problemTextVarNum1>3</problemTextVarNum1>
    </filter>
    <filter>
      <name>bwSMDIOperationFailure</name>
      <active>true</active>
      <maxNumTrapsPerTimePeriod>10</maxNumTrapsPerTimePeriod>
      <timePeriodInSeconds>60</timePeriodInSeconds>
      <problemTextVarNum1>2</problemTextVarNum1>
      <problemTextVarNum2>3</problemTextVarNum2>
    </filter>
  </trapFilter>
```

The Application Server SNMP agent filters faults as follows:

- In general, no more than 10 faults of a type per sliding period of five seconds are sent out over the SNMP interface, unless fault-specific filters exist for some faults. However, this system default threshold is inactive, so the SNMP agent simply ignores this threshold definition. Also, if the default fault filter is activated, only faults with a severity of *low* (1) or greater are sent out. Informational faults are discarded.
- All *bwSipRegistrationFailure* faults are filtered out and none are sent over the SNMP interface.
- The SNMP agent only sends a maximum of two *bwSipUnexpectedMessage* faults per sliding period of five seconds.
- For a given Network Server address (<problemTextVarNum1>3</problemTextVarNum1>), the SNMP agent sends a maximum of one *bwNSSynchronizationFailure* fault per sliding period of ten seconds.
- For a given phone number (<problemTextVarNum1>2</problemTextVarNum1>) and a given failure reason (<problemTextVarNum2>3</problemTextVarNum2>), the SNMP agent sends a maximum of ten bwSMDIOperationFailure faults per sliding period of one minute.

The above feature behavior is the same on all types of BroadWorks servers.

6.3 Filtering Considerations

- Cisco does not provide any predefined fault suppression or threshold rules in the various trapfilter files besides the system default fault threshold (set to "inactive").
- Fault filtering works on a per-node basis and not on a per-cluster basis. This means that if a filter specifies that fault X should be discarded if the generation rate exceeds five faults per second, no fault is discarded if each server in a cluster has an actual rate of three faults per second, even though the aggregated rate for this two-node cluster is actually of six faults per second.
- The data that the SNMP agent uses to filter out faults is not persisted. This means that after the SNMP agent restarts, filtering is reinitialized using the filters defined in the trapfilter file, and faults are sent out until the various thresholds are reached once more.
- For a given fault name, it is possible to define more than one filter. In this case, all filters are evaluated and if at least one does not allow the fault to be sent, then the fault is not sent.
- If *maxNumTrapsPerTimePeriod* is set to *0* (zero) or a negative integer value, then the fault (matching the other filter criteria, if some are specified) is suppressed. In such a case, the timePeriodInSeconds value is ignored.
- If *maxNumTrapsPerTimePeriod* is a positive integer greater than zero, then the fault (matching the other filter criteria, if some are specified) has a threshold. In such a case, the *timePeriodInSeconds* must contain a positive integer value greater than zero.
- Fault threshold uses the concept of sliding time period. When the agent receives a fault, it checks how many alarms matching the threshold rule(s) were received in the previous *timePeriodInSeconds* seconds. If that number exceeds *maxNumTrapsPerTimePeriod*, then the alarm is not sent over the SNMP interface. The agent remembers that this fault was received, for proper filtering when the next one comes.
- A maximum of five problem text variable filters can be defined per threshold. When the agent compares the content of problem text variables for filtering purposes, the comparison is not case sensitive.

- If a fault filter is provisioned with an invalid fault name (that is, the fault name does not exist in the system), the filter is accepted but it remains in state invalid.
- If the filtered fault is an alarm, the alarm is still added to the Alarms table.

6.4 Filtered Faults Notification

The fault named *bwAlarmsDiscarded* is common to all servers. The SNMP agent generates this fault every 15 minutes (15 minutes after SNMP agent restart and every 15 minutes thereafter) if at least one fault was discarded in the past 15 minutes. If this is the case, the fault gives a list of all the alarms that were discarded in the past 15 minutes along with the number of times each fault was discarded.

If the data to be included in the alarm gets too big, more than one fault is generated. The threshold is set to no more than 1024 characters in the list (and count) of faults discarded.

6.5 Provisioning Fault Filters

The SNMP agent stores all fault filters in a trapfilter file, as described in the previous sections. To provision fault filters, an administrator can:

- Use the SNMP interface to ask the SNMP agent to add, delete, get, and set fault filters.
- Use the Cisco BroadWorks CLI interface to add, delete, get, and set fault filters.

These methods are explained in detail in the following subsections.

6.5.1 SNMP Provisioning

The definition of fault filters and their configuration are part of the BroadworksMaintenance.mib. Therefore, any network element that has an authorized SNMP connectivity to the server's SNMP agent can configure fault filters. Fault filters can only be provisioned if the SNMP agent is running.

6.5.2 CLI Provisioning

It is also possible to add, delete, get, and set fault filters using the Cisco BroadWorks CLI. To provision and configure fault filters using the CLI, the SNMP agent on the server must be running. The following is an example (on an Application Server) showing how fault filters can be managed using the CLI.

```
AS_CLI/Monitoring/Alarm/Threshold> get
  Index  AlarmName  MaxNumTrapsPerTimePeriod  TimePeriodInSeconds
  Var1  Var2  Var3  Var4  Var5  Status
=====================================================================
=====================================

0 entry found.

AS_CLI/Monitoring/Alarm/Threshold> %% No more than 4 bwNSSynchronizationFailure alarms
 per sliding period of 10 seconds.

AS_CLI/Monitoring/Alarm/Threshold> add bwNSSynchronizationFailure 4 10 active
...Done

AS_CLI/Monitoring/Alarm/Threshold> %% Suppress all bwSipRegistrationFailure alarms.

AS_CLI/Monitoring/Alarm/Threshold> add bwSipRegistrationFailure 0 1 active
...Done

AS_CLI/Monitoring/Alarm/Threshold/Default> %% Limit each alarm in system to 100 alarms
 of each type per hour.

AS_CLI/Monitoring/Alarm/Threshold/Default> set maxNumTrapsPerTimePeriod 100
 timePeriodInSeconds 3600 status active minSeverity low
```

```
...Done

AS_CLI/Monitoring/Alarm/Threshold> %% For the same Endpoint ID (problem text variable
 position 1) and Device Address (problem text variable position 2), limit the number of
 bwMGCPReTransmissionTimeout alarms to 2 per sliding period of 30 seconds.

AS_CLI/Monitoring/Alarm/Threshold> add bwMGCPReTransmissionTimeout 2 30 active
 problemTextVariable1 1 problemTextVariable2 2
...Done

AS_CLI/Monitoring/Alarm/Threshold> get
  Index                    AlarmName  MaxNumTrapsPerTimePeriod  TimePeriodInSeconds
Var1  Var2  Var3  Var4  Var5  Status
================================================================================
==================================
      1   bwNSSynchronizationFailure                        4                   10

                             active
      2     bwSipRegistrationFailure                        0                    1

                             active
      4  bwMGCPReTransmissionTimeout                        2                   30
      1     2                 active

3 entries found.

AS_CLI/Monitoring/Alarm/Threshold/Default> get
  maxNumTrapsPerTimePeriod = 100
  timePeriodInSeconds = 3600
  status = active
  minSeverity = low
```

7 Organization of Cisco BroadWorks MIB Files

This section describes the organization of Cisco BroadWorks MIB files by server type. In addition, the range of notification OIDs currently in use by each MIB file is identified.

NOTE: fault IDs are uniquely defined within Cisco BroadWorks. All faults have the following root OID:

.1.3.6.1.4.1.6431.1.1.1

You can click on the link of each MIB for a description of the MIB.

7.1 MIB files for the Network Server

MIB files for the Network Server.

Table 12: MIB Files and OID Value Ranges for the Network Server.

MIB File	Application	Notification ID Range
BroadworksConfigurationFault MIB	BroadWorks Platform	6101 through 6109
BroadworksFault MIB		2 through 11759
BW-LicenseManagerFault MIB		15801 through 15813
BW-NSExecutionFault MIB	NS Execution And Provisioning Application	1001 through 1049
BW-NSProvisioningFault MIB		1005 through 1306
BW-NSPortalFault MIB	NS Portal Application	1036 through 1251
BW-WebContainerFault MIB	Web Container Application	6001 through 6013

8 Cisco BroadWorks MIB Files

This section describes all Cisco BroadWorks MIBs in alphabetical order.

8.1 BroadworksConfigurationFault MIB

This section presents SNMP traps (notifications and alarms) for the BroadworksConfigurationFault MIB grouped by component.

The MIB defines the faults for the Configuration subsystem.

Applicable server(s):

Network Server.

8.1.1 SNMP Traps For Component: processmonitor

The table that follows describes the SNMP traps for the processmonitor subcomponent of the BroadworksConfigurationFault MIB.

Table 13: SNMP Traps For BroadworksConfigurationFault:processmonitor

Alarm Name	Attributes	Values
bwPMconfigdLaunched	Problem Type	Notification
	OID	6101
	Status	current
	Severity Range	informational
	Description	This notification indicates that the configuration agent has been started.
	Problem Text	configd started.
	Recommended Action(s)	
	Correlation Rules	bwPMconfigdLaunched, bwPMconfigdShutDown, bwPMconfigdRestarted, and bwPMconfigdDeath can be correlated into a single alarm. These events have to be considered as a transition of the state machine for the management of the configd process.
bwPMconfigdShutDown	Problem Type	Notification
	OID	6102
	Status	current
	Severity Range	informational
	Description	This notification indicates that the configuration agent has been shutdown.
	Problem Text	configd shutdown.
	Recommended Action(s)	
	Correlation Rules	bwPMconfigdLaunched, bwPMconfigdShutDown, bwPMconfigdRestarted, and bwPMconfigdDeath can be correlated into a single alarm. These events have to be considered as a transition of the state machine for the management of the configd process.

Alarm Name	Attributes	Values
bwPMconfigdRestarted	Problem Type	Notification
	OID	6103
	Status	current
	Severity Range	informational
	Description	This notification indicates that the configuration agent has been restarted.
	Problem Text	configd restarted.
	Recommended Action(s)	
	Correlation Rules	bwPMconfigdLaunched, bwPMconfigdShutDown, bwPMconfigdRestarted, and bwPMconfigdDeath can be correlated into a single alarm. These events have to be considered as a transition of the state machine for the management of the configd process.
bwPMconfigdDeath	Problem Type	Notification
	OID	6104
	Status	current
	Severity Range	critical
	Description	This notification indicates that the configuration agent as abnormally terminated.
	Problem Text	configd terminated.
	Recommended Action(s)	Make sure configd gets restarted
	Correlation Rules	bwPMconfigdLaunched, bwPMconfigdShutDown, bwPMconfigdRestarted, and bwPMconfigdDeath can be correlated into a single alarm. These events have to be considered as a transition of the state machine for the management of the configd process.

8.1.2 SNMP Traps For Component: configd

The table that follows describes the SNMP traps for the configd subcomponent of the BroadworksConfigurationFault MIB.

Table 14: SNMP Traps For BroadworksConfigurationFault:configd

Alarm Name	Attributes	Values
bwConfigurationChanged	Problem Type	Notification
	OID	6105
	Status	current
	Severity Range	informational
	Description	This notification indicates that the configuration agent as loaded a new configuration version.
	Problem Text	Configuration version %npConfigVersion% loaded.
	Recommended Action(s)	

Alarm Name	Attributes	Values
	Correlation Rules	
bwConfigurationFailed	Problem Type	Notification
	OID	6106
	Status	current
	Severity Range	high
	Description	This notification indicates that the configuration agent as failed to loaded a new configuration version.
	Problem Text	Configuration version %npConfigVersion% failed.
	Recommended Action(s)	
	Correlation Rules	
bwConfigReplicationOffline	Problem Type	Alarm
	OID	6108
	Status	current
	Severity Range	high
	Description	This alarm indicates that the configuration replication is currently offline.
	Problem Text	Configuration replication is offline.
	Recommended Action(s)	
	Correlation Rules	
bwConfigReplicationFailed	Problem Type	Notification
	OID	6109
	Status	current
	Severity Range	high
	Description	This notification indicates that the master's configuration could not be properly replicated.
	Problem Text	The master's configuration could not be properly replicated.
	Recommended Action(s)	
	Correlation Rules	

8.2 BroadworksFault MIB

This section presents SNMP traps (notifications and alarms) for the BroadworksFault MIB grouped by component.

This MIB defines management information that is common to all elements in a Broadworks system.

Applicable server(s):

Network Server.

8.2.1 SNMP Traps For Component: unspecified

The table that follows describes the SNMP traps for the unspecified subcomponent of the BroadworksFault MIB.

Table 15: SNMP Traps For BroadworksFault:unspecified

Alarm Name	Attributes	Values
bwGeneralSoftwareError	Problem Type	Notification
	OID	5
	Status	current
	Severity Range	medium-high
	Description	This software error indicates that an unspecified software error has occurred.
	Problem Text	Unexpected software error occurred during processing. Stack Trace: %npStackTrace%
	Recommended Action(s)	Contact BroadSoft Support Engineer.
	Correlation Rules	
bwServerStateTransition	Problem Type	Notification
	OID	12
	Status	current
	Severity Range	informational
	Description	Reports a BroadWorks server state transition.
	Problem Text	Server administrative state change. Old Administrative State: %npOldAdministrativeState%, New Administrative State: %npNewAdministrativeState%
	Recommended Action(s)	
	Correlation Rules	It is recommended to clear all alarms associated with a network element whenever there is an NE transition to the enable state, since the network element, itself, will in this case automatically clear all internal error conditions.
bwAlarmsDiscarded	Problem Type	Notification
	OID	41
	Status	current
	Severity Range	low
	Description	Provides a complete list of all the alarms that the SNMP agent discarded in the past 15 minutes either because they are suppressed or because they exceeded their predefined threshold criteria.
	Problem Text	The following alarms were discarded during the 15 minutes period ending at: %npTimestamp% %npAlarmList%

Alarm Name	Attributes	Values
	Recommended Action(s)	
	Correlation Rules	
bwApplicationStateTransition	Problem Type	Notification
	OID	52
	Status	current
	Severity Range	informational
	Description	Reports an application's administrative or effective state transition.
	Problem Text	Application State Changed Application Name: %npApplicationName%, Old Administrative State: %npOldAdministrativeState%, New Administrative State: %npNewAdministrativeState%, Old Effective State: %npOldEffectiveState%, New Effective State: %npNewEffectiveState%
	Recommended Action(s)	
	Correlation Rules	
bwExtremeOverload	Problem Type	Notification
	OID	80
	Status	current
	Severity Range	high
	Description	Queue dropped event because of extreme overload.
	Problem Text	Queue dropped event because of extreme overload. Queue name: %npQueueName% Reason: %npExtremeOverloadReason%
	Recommended Action(s)	
	Correlation Rules	
bwCPEDeviceConfigurationDeviceReset	Problem Type	Notification
	OID	3572
	Status	current
	Severity Range	medium
	Description	An IP phone could not be reset.
	Problem Text	An IP phone could not be reset. Device Name: %npDeviceName% Remote Host: %npRemoteAddress%

Alarm Name	Attributes	Values
	Recommended Action(s)	Use one of the following steps to troubleshoot the problem: 1- Check that the phone is on, or 2- Check that the communication to the phone is up.
	Correlation Rules	

8.2.2 SNMP Traps For Component: processmonitor

The table that follows describes the SNMP traps for the processmonitor subcomponent of the BroadworksFault MIB.

Table 16: SNMP Traps For BroadworksFault:processmonitor

Alarm Name	Attributes	Values
bwPMtomcatLaunched	Problem Type	Notification
	OID	6
	Status	current
	Severity Range	informational
	Description	This notification indicates that the Tomcat server has been started.
	Problem Text	tomcat started.
	Recommended Action(s)	
	Correlation Rules	bwPMtomcatLaunched, bwPMtomcatShutDown, bwPMtomcatStarted, and bwPMtomcatDeath can be correlated into a single notification. These events have to be considered as a transition of the state machine for the management of the Tomcat process running on some of the BroadWorks servers.
bwPMtomcatShutDown	Problem Type	Notification
	OID	7
	Status	current
	Severity Range	informational
	Description	This notification indicates that the Tomcat server has been manually shut down.
	Problem Text	tomcat shut down.
	Recommended Action(s)	
	Correlation Rules	bwPMtomcatLaunched, bwPMtomcatShutDown, bwPMtomcatStarted, and bwPMtomcatDeath can be correlated into a single notification. These events have to be considered as a transition of the state machine for the management of the Tomcat process running on some of the BroadWorks servers.
bwPMtomcatRestarted	Problem Type	Notification
	OID	8
	Status	current
	Severity Range	informational

Alarm Name	Attributes	Values
	Description	This notification provides the date and time of the Tomcat server restart.
	Problem Text	tomcat restarted.
	Recommended Action(s)	Log in BroadWorks.
	Correlation Rules	bwPMtomcatLaunched, bwPMtomcatShutDown, bwPMtomcatStarted, and bwPMtomcatDeath can be correlated into a single notification. These events have to be considered as a transition of the state machine for the management of the Tomcat process running on some of the BroadWorks servers.
bwPMtomcatDeath	Problem Type	Notification
	OID	9
	Status	current
	Severity Range	critical
	Description	This notification provides the date and time of the Tomcat server death.
	Problem Text	tomcat terminated.
	Recommended Action(s)	Make sure tomcat gets restarted
	Correlation Rules	bwPMtomcatLaunched, bwPMtomcatShutDown, bwPMtomcatStarted, and bwPMtomcatDeath can be correlated into a single notification. These events have to be considered as a transition of the state machine for the management of the Tomcat process running on some of the BroadWorks servers.
bwSystemHealthReport	Problem Type	Notification
	OID	10
	Status	current
	Severity Range	informational-critical
	Description	System health report. See Appendix B of the BroadWorks Faults and Alarms Interface Specification for a description of the bwSystemHealthReport Alarm Problem Text.
	Problem Text	%npReport%
	Recommended Action(s)	*
	Correlation Rules	The system health should always be at the latest state/severity reported by a bwSystemHealthReport trap. For example a critical alarm raised through bwSystemHealthReport could be cleared automatically in case the next severity received is informational.
bwDatabaseSyncReport	Problem Type	Notification
	OID	11
	Status	current
	Severity Range	informational

Alarm Name	Attributes	Values
	Description	This notification is generated by the synchcheck_basic.pl command. It provides a detail reports on database differences.
	Problem Text	%npReport%
	Recommended Action(s)	*
	Correlation Rules	
bwCPUIdleTimeLimitReached	Problem Type	Notification
	OID	17
	Status	current
	Severity Range	informational-critical
	Description	CPU idle time monitoring.
	Problem Text	Average CPU idle time is %npCpuIdleTimePercentage %% where the %npThresholdName% threshold is %npCurrentThresholdValue%%
	Recommended Action(s)	This may be an intermittent issue. Verify by performing the following: - Monitor real-time server CPU usage using "vmstat 1 10". - Identify high running process using "top". - If "sar" is enabled, check historic CPU usage statistics. If high CPU usage persists, issue the following command and send the output to BroadSoft support: $ tech-support
	Correlation Rules	It is recommended to always keep the highest severity value for this notification until it is cleared.
bwMemoryLimitReached	Problem Type	Notification
	OID	18
	Status	current
	Severity Range	critical
	Description	This notification is generated by the bwCPUMon script. It monitors the heap, CPU, and I/O usage for the entire system and for the Execution Server process (Application Server only).
	Problem Text	%npReport%
	Recommended Action(s)	Issue the following command and send the output to BroadSoft support: $ tech-support
	Correlation Rules	It is recommended to always keep the highest severity value for this notification until it is cleared.
bwPMremotexlaLaunched	Problem Type	Notification
	OID	21
	Status	current
	Severity Range	informational

Alarm Name	Attributes	Values
	Description	This notification indicates that the remote XLA server has been started.
	Problem Text	remotexla started.
	Recommended Action(s)	
	Correlation Rules	bwPMremotexlaLaunched, bwPMremotexlaShutDown, bwPMremotexlaRestarted, and bwPMremotexlaDeath can be correlated into a single notification. These events have to be considered as a transition of the state machine for the management of the remoteXLA process running on some of the BroadWorks servers.
bwPMremotexlaShutDown	Problem Type	Notification
	OID	22
	Status	current
	Severity Range	informational
	Description	This notification indicates that the remote XLA server has been manually shut down.
	Problem Text	remotexla shut down.
	Recommended Action(s)	
	Correlation Rules	bwPMremotexlaLaunched, bwPMremotexlaShutDown, bwPMremotexlaRestarted, and bwPMremotexlaDeath can be correlated into a single notification. These events have to be considered as a transition of the state machine for the management of the remoteXLA process running on some of the BroadWorks servers.
bwPMremotexlaRestarted	Problem Type	Notification
	OID	23
	Status	current
	Severity Range	informational
	Description	This notification provides the date and time of the remote XLA server restart.
	Problem Text	remotexla restarted.
	Recommended Action(s)	Log in BroadWorks.
	Correlation Rules	bwPMremotexlaLaunched, bwPMremotexlaShutDown, bwPMremotexlaRestarted, and bwPMremotexlaDeath can be correlated into a single notification. These events have to be considered as a transition of the state machine for the management of the remoteXLA process running on some of the BroadWorks servers.
bwPMremotexlaDeath	Problem Type	Notification
	OID	24
	Status	current
	Severity Range	critical

Alarm Name	Attributes	Values
	Description	This notification provides the date and time of the remote XLA server death.
	Problem Text	remotexla terminated.
	Recommended Action(s)	Make sure remotexla gets restarted
	Correlation Rules	bwPMremotexlaLaunched, bwPMremotexlaShutDown, bwPMremotexlaRestarted, and bwPMremotexlaDeath can be correlated into a single notification. These events have to be considered as a transition of the state machine for the management of the remoteXLA process running on some of the BroadWorks servers.
bwPMhttpdLaunched	Problem Type	Notification
	OID	48
	Status	current
	Severity Range	informational
	Description	Apache started.
	Problem Text	apache started.
	Recommended Action(s)	
	Correlation Rules	
bwPMhttpdShutDown	Problem Type	Notification
	OID	49
	Status	current
	Severity Range	informational
	Description	Apache manually shut down.
	Problem Text	apache shut down.
	Recommended Action(s)	
	Correlation Rules	
bwPMhttpdRestarted	Problem Type	Notification
	OID	50
	Status	current
	Severity Range	informational
	Description	Apache restarted.
	Problem Text	apache restarted.
	Recommended Action(s)	Log in BroadWorks.
	Correlation Rules	
bwPMhttpdDeath	Problem Type	Notification
	OID	51

Alarm Name	Attributes	Values
	Status	current
	Severity Range	critical
	Description	Apache process unexpectedly died.
	Problem Text	apache terminated.
	Recommended Action(s)	Make sure apache gets restarted
	Correlation Rules	
bwMaintenanceTaskFailure	Problem Type	Notification
	OID	65
	Status	current
	Severity Range	medium
	Description	A maintenance task failed to execute.
	Problem Text	The maintenance task %npTaskName% failed to execute
	Recommended Action(s)	*
	Correlation Rules	
bwSystemBackwardTimeDrift	Problem Type	Notification
	OID	73
	Status	current
	Severity Range	high
	Description	The system time has gone backward, which can result in software malfunction.
	Problem Text	The system time has gone backward, which can result in software malfunction.
	Recommended Action(s)	Verify that BroadWorks applications are working as expected, if this is not the case, restart BroadWorks.
	Correlation Rules	
bwOSMisconfiguration	Problem Type	Notification
	OID	90
	Status	current
	Severity Range	high-critical
	Description	This notification indicates that an OS parameter is not set to recommended value.
	Problem Text	Problem detail: %npMessage%
	Recommended Action(s)	*
	Correlation Rules	

8.2.3 SNMP Traps For Component: database

The table that follows describes the SNMP traps for the database subcomponent of the BroadworksFault MIB.

Table 17: SNMP Traps For BroadworksFault:database

Alarm Name	Attributes	Values
bwCentralizedDatabaseConnectivity Failure	Problem Type	Alarm
	OID	60
	Status	current
	Severity Range	high
	Description	A connectivity failure is detected on the connection to a centralized database site for a given site.
	Problem Text	A connectivity failure occurred for Database %npDatabaseName % on site %npSite%.
	Recommended Action(s)	Verify that the Database Server(s) on the problematic sites are running and verify the IP connectivity between the local node to the Database Server site on the configured port.
	Correlation Rules	
bwCentralizedDatabaseSchemaFailure	Problem Type	Alarm
	OID	67
	Status	current
	Severity Range	high
	Description	A schema access failure is detected to a centralized database site for a given schema.
	Problem Text	A schema access failure occurred for schema %npSchemaInstanceName% (state = %npSchemaInstanceState%).
	Recommended Action(s)	Make sure the application is connected to a Read/Write Centralized Database site.
	Correlation Rules	
bwNetworkDatabaseNodeConnectivity Failure	Problem Type	Alarm
	OID	77
	Status	current
	Severity Range	high
	Description	This notification indicates that the application has no connectivity to a database node.
	Problem Text	A connectivity failure is detected on the connection to a Network Database node: Database: %npDatabaseName% Node: %npDatabaseNode%.
	Recommended Action(s)	Verify that the Network Database node is running and verify the IP connectivity between the server reporting the fault and the database node. Verify the database node hostname and port configuration.

Alarm Name	Attributes	Values
	Correlation Rules	
bwNetworkDatabaseClusterConnectivityFailure	Problem Type	Alarm
	OID	78
	Status	current
	Severity Range	critical
	Description	This notification indicates that the application has no connectivity to all the database nodes.
	Problem Text	Connectivity lost with all the Network Database nodes for database %npDatabaseName% Nodes: %npDatabaseNode%.
	Recommended Action(s)	Verify that the Network Database nodes are running and verify the IP connectivity between the server reporting the fault and all the database nodes. Verify the database nodes hostname and port configuration.
	Correlation Rules	
bwNetworkDatabaseSchemaFailure	Problem Type	Alarm
	OID	79
	Status	current
	Severity Range	high
	Description	This notification indicates that a schema instance is not able to communicate to any node of the Network Database.
	Problem Text	A schema access failure is detected to Network Database %npDatabaseName% for schema instance %npSchemaInstanceName%.
	Recommended Action(s)	Verify that the Network Database nodes are running and verify the IP connectivity between the server reporting the fault and all the database nodes. Verify the database nodes hostname and port configuration. Verify the schema instance configuration to make sure it uses the correct database. Verify if the schema instance is in state OFFLINE in the Network Database.
	Correlation Rules	
bwCouchbaseNodeConnectivityFailure	Problem Type	Alarm
	OID	81
	Status	current
	Severity Range	low, high, critical
	Description	This notification indicates that the application has no connectivity to one or more Couchbase nodes.
	Problem Text	A connectivity failure is detected on the connection to one or more Couchbase nodes: Node(s): %npCouchbaseNodes%
	Recommended Action(s)	
	Correlation Rules	

Alarm Name	Attributes	Values
bwCentralizedDatabaseListenerFailure	Problem Type	Alarm
	OID	82
	Status	current
	Severity Range	high
	Description	Cannot connect to Oracle Database Listener.
	Problem Text	A failure occured connecting to listener at %npAddress%.
	Recommended Action(s)	Make sure the listener is working properly on Database site
	Correlation Rules	
bwCentralizedDatabaseMaxConnections Reached	Problem Type	Alarm
	OID	83
	Status	current
	Severity Range	high
	Description	Maximum number of borrowable connections has been reached.
	Problem Text	Maximum number of borrowable connections has been reached (%npConnectionCount% connections)
	Recommended Action(s)	
	Correlation Rules	
bwCentralizedDatabaseNewConnection Failure	Problem Type	Alarm
	OID	84
	Status	current
	Severity Range	high
	Description	Unable to create a new database connection.
	Problem Text	The persistency monitoring framework failed to create a new database connection on %npSite%
	Recommended Action(s)	Make sure all listeners are working and responsive on Database site
	Correlation Rules	
bwCentralizedDatabasePoolFailure	Problem Type	Alarm
	OID	87
	Status	current
	Severity Range	critical
	Description	Cannot initialize the specified connection pool, reducing the initPoolSize and restarting the application is required.
	Problem Text	Cannot initialize the %npConnectionPoolName% connection pool.
	Recommended Action(s)	Reduce the value of the initPoolSize parameter and restart the application to free connections.

Alarm Name	Attributes	Values
	Correlation Rules	

8.2.4 SNMP Traps For Component: sip

The table that follows describes the SNMP traps for the sip subcomponent of the BroadworksFault MIB.

Table 18: SNMP Traps For BroadworksFault:sip

Alarm Name	Attributes	Values
bwSipTcpExceededMax	Problem Type	Notification
	OID	31
	Status	current
	Severity Range	low
	Description	SIP TCP connections reclaimed to avoid exceeding the maximum number of SIP TCP connections.
	Problem Text	SIP TCP connections reclaimed to avoid exceeding the maximum number of SIP TCP connections.
	Recommended Action(s)	No action is typically required. Adjust the following configuration values as needed: maxNumberTcpSocketsPerSystem, autoDiscardStaleConnections, and staleConnectionTimerInMinutes.
	Correlation Rules	
bwSipTcpExceededMaxPerPeer	Problem Type	Notification
	OID	32
	Status	current
	Severity Range	low
	Description	SIP TCP connections associated with the IP address were reclaimed to avoid exceeding the maximum number of SIP TCP connections per peer.
	Problem Text	SIP TCP connections associated with %npRemoteAddress% were reclaimed to avoid exceeding the maximum number of SIP TCP connections per peer.
	Recommended Action(s)	No action is typically required. Adjust the following configuration values as needed: maxNumberTcpSocketsPerPeer, autoDiscardStaleConnections, and staleConnectionTimerInMinutes.
	Correlation Rules	
bwSipTcpSocketError	Problem Type	Notification
	OID	33
	Status	current
	Severity Range	low
	Description	SIP TCP connection associated with IP address and port was released or unable to be established
	Problem Text	SIP TCP connection associated with %npRemoteAddress% was released or unable to be established.

Alarm Name	Attributes	Values
	Recommended Action(s)	
	Correlation Rules	
bwSipSocketAlreadyBound	Problem Type	Notification
	OID	71
	Status	current
	Severity Range	low
	Description	The server attempted to bind a socket against a local port that was already used.
	Problem Text	Could not bind to %npLocalPort%
	Recommended Action(s)	
	Correlation Rules	
bwSipMessageParsingError	Problem Type	Notification
	OID	3509
	Status	current
	Severity Range	low
	Description	This notification indicates that BroadWorks is unable to parse an incoming SIP message.
	Problem Text	Unable to parse SIP message. Error is %npMissingHeader%. Message: %npMessage%
	Recommended Action(s)	Check SIP message for syntax error
	Correlation Rules	
bwSipRegistrationFailure	Problem Type	Notification
	OID	3510
	Status	current
	Severity Range	low
	Description	This notification indicates that BroadWorks rejected a registration attempt from an endpoint due to the Emergency Zone feature.
	Problem Text	Emergency Zone rejected SIP Registration. Message: %npMessage%
	Recommended Action(s)	
	Correlation Rules	
bwSipUnexpectedMessage	Problem Type	Notification
	OID	3511
	Status	current

Alarm Name	Attributes	Values
	Severity Range	low
	Description	This notification indicates that an unexpected SIP message is received.
	Problem Text	Unexpected SIP Message received. Reason: %npReason% Response Message: %npSipResponseMessage% Request Message: %npSipRequestMessage%
	Recommended Action(s)	
	Correlation Rules	
bwSipMaxRetriesExceeded	Problem Type	Notification
	OID	3512
	Status	current
	Severity Range	low
	Description	This notification indicates a SIP request was aborted after maximum number of retries.
	Problem Text	SIP request %npMethod% aborted after maximum number of retries. Call-ID: %npCallId% Destination address: %npDeviceAddress%:%npRemotePort%
	Recommended Action(s)	
	Correlation Rules	
bwSipRequestTimeOutReceived	Problem Type	Notification
	OID	3513
	Status	current
	Severity Range	low
	Description	This notification indicates that a SIP request timeout message was received.
	Problem Text	SIP respond 408 Request Timeout received. Response Message: %npSipResponseMessage% Request Message: %npSipRequestMessage% Device Address: %npDeviceAddress%
	Recommended Action(s)	
	Correlation Rules	

Alarm Name	Attributes	Values
bwSipServiceUnavailableReceived	Problem Type	Notification
	OID	3514
	Status	current
	Severity Range	low
	Description	This notification indicates that a SIP service unavailable message was received.
	Problem Text	SIP respond 503 Service Unavailable received. Response Message: %npSipResponseMessage% Request Message: %npSipRequestMessage% Device Address: %npDeviceAddress%
	Recommended Action(s)	
	Correlation Rules	
bwSipServerTimeOutReceived	Problem Type	Notification
	OID	3515
	Status	current
	Severity Range	low
	Description	This notification indicates that a SIP server timeout message was received.
	Problem Text	SIP respond 504 Server Timeout received. Response Message: %npSipResponseMessage% Request Message: %npSipRequestMessage% Device Address: %npDeviceAddress%
	Recommended Action(s)	
	Correlation Rules	
bwAclViolation	Problem Type	Notification
	OID	3517
	Status	current
	Severity Range	low
	Description	SIP request received from an unknown device.
	Problem Text	SIP request %npMethod% received violates access control list. Call-ID: %npCallId% %npReason%
	Recommended Action(s)	

Alarm Name	Attributes	Values
	Correlation Rules	
bwSipUnrecognisedDomainName	Problem Type	Notification
	OID	3518
	Status	current
	Severity Range	medium
	Description	The domain name entered in the access device location is unrecognized or the domain name server is unreachable.
	Problem Text	The access device:%npHost% is not currently in service
	Recommended Action(s)	Check the connectivity/availability of the DNS or verify the domain name used as location.
	Correlation Rules	
bwSipTcpConnectionFailure	Problem Type	Notification
	OID	3595
	Status	current
	Severity Range	low
	Description	Failure to establish TCP connection.
	Problem Text	Could not connect to %npRemoteAddress%
	Recommended Action(s)	Check the connectivity, availability, and configuration of the device.
	Correlation Rules	

8.2.5 SNMP Traps For Component: mgcp

The table that follows describes the SNMP traps for the mgcp subcomponent of the BroadworksFault MIB.

There is no visible fault for this component.

8.2.6 SNMP Traps For Component: smtp

The table that follows describes the SNMP traps for the smtp subcomponent of the BroadworksFault MIB.

Table 19: SNMP Traps For BroadworksFault:smtp

Alarm Name	Attributes	Values
bwSMTPPrimaryServerEmailMessage DeliveryError	Problem Type	Alarm
	OID	3519
	Status	current
	Severity Range	low
	Description	This notification indicates that the system failed to deliver an e-mail message via the primary SMTP server.
	Problem Text	System failed to deliver emails via the primary SMTP server.
	Recommended Action(s)	Check the connectivity/availability of the primary SMTP server.
	Correlation Rules	

Alarm Name	Attributes	Values
bwSMTPConnectivityFailure	Problem Type	Notification
	OID	3520
	Status	current
	Severity Range	high
	Description	This notification indicates that the system has lost the connection to both SMTP servers.
	Problem Text	System failed to deliver emails via the primary and the secondary SMTP servers.
	Recommended Action(s)	Check the connectivity/availability of the primary and secondary SMTP servers.
	Correlation Rules	

8.2.7 SNMP Traps For Component: filesystem

The table that follows describes the SNMP traps for the filesystem subcomponent of the BroadworksFault MIB.

Table 20: SNMP Traps For BroadworksFault:filesystem

Alarm Name	Attributes	Values
bwFileServerClusterUnreachable	Problem Type	Alarm
	OID	37
	Status	current
	Severity Range	critical
	Description	The file server cluster is unreachable, causing a file operation to fail.
	Problem Text	Could not connect to any server in file server cluster %npClusterName%.
	Recommended Action(s)	Verify that: - The file server is properly configured in CLI context System/MediaFileSystem and/or in CLI context System/Device/FileRepos. - The DNS is properly configured. - The failing file server nodes are reachable from the Application Server, the Media Server and the Xtended Services Platform for device management. - The file server is properly configured.
	Correlation Rules	
bwFileServerNodeUnreachable	Problem Type	Notification
	OID	38
	Status	current
	Severity Range	high
	Description	One node in the file server cluster is not reachable.

Alarm Name	Attributes	Values
	Problem Text	The file server node %npRemoteAddress% in the file server cluster %npClusterName% is unreachable.
	Recommended Action(s)	Verify that: - The DNS is properly configured for the failing file server nodes. - The failing file server nodes are reachable from the Application Server, the Media Server and/or the Xtended Services Platform for device management. - The file server is properly configured on the failing file server nodes.
	Correlation Rules	

8.2.8 SNMP Traps For Component: callp

The table that follows describes the SNMP traps for the callp subcomponent of the BroadworksFault MIB.

Table 21: SNMP Traps For BroadworksFault:callp

Alarm Name	Attributes	Values
bwCongestionManagementNeighborsInhibited	Problem Type	Notification
	OID	46
	Status	current
	Severity Range	medium
	Description	The Application Server has identified the main overload source when it enters into the yellow zone.
	Problem Text	%npNbInhibitedNeighbors% network element addresses caused the server to become overloaded: %npInhibitedNeighbors%
	Recommended Action(s)	
	Correlation Rules	
bwAuditAbnormalCallTermination	Problem Type	Notification
	OID	3536
	Status	current
	Severity Range	low
	Description	This notification is sent when an end device does not respond during an active call or when a call is detected in the system in an incorrect state. Session audit has terminated the call when this alarm is sent.
	Problem Text	Failed audit User: %npUserUid% Session Key: %npSessionKey% Endpoint: %npEndpointId%
	Recommended Action(s)	None
	Correlation Rules	
bwCallPThreadAutoRestart	Problem Type	Notification

Alarm Name	Attributes	Values
	OID	3555
	Status	current
	Severity Range	high
	Description	This notification is sent when the Application Server call processing watchdog thread has detected a problem with a call processing thread and has restarted it.
	Problem Text	Thread automatically restarted by watchdog: %npThreadName%
	Recommended Action(s)	Contact Broadsoft support.
	Correlation Rules	
bwForcedExitDueToHungThread	Problem Type	Notification
	OID	3556
	Status	current
	Severity Range	critical
	Description	This notification is sent when the Application Server call processing watchdog thread has detected a problem with a call processing thread. An attempt was made to restart the thread, however this has failed. The Application Server processes exits and is restarted by the process monitor.
	Problem Text	Application server restarting because of unrecoverable problem in thread: %npThreadName%
	Recommended Action(s)	Check log file for full Java stack trace and contact Broadsoft support.
	Correlation Rules	
bwThreadDelayDetected	Problem Type	Notification
	OID	3594
	Status	current
	Severity Range	high
	Description	A thread was delayed.
	Problem Text	The %npThreadName% thread was delayed for %npTimeElapsed% milliseconds. A thread dump is available in the XSOutput log file. Last message processed: %npMessage%
	Recommended Action(s)	Contact Broadsoft support and supply the XSOutput file.
	Correlation Rules	
bwPhysicalLocationOriginationBlocked	Problem Type	Notification
	OID	3609
	Status	current
	Severity Range	informational

Alarm Name	Attributes	Values
	Description	User origination blocked by the Physical Location service.
	Problem Text	User origination blocked by the Physical Location service. User ID: %npUserId% Call ID: %npCallId% Dialed Number: %npDialedNumber% Device Line/Port: %npDeviceLinePort% Received Physical Location: %npReceivedPhysicalLocation% Configured Physical Location: %npConfiguredPhysicalLocation%
	Recommended Action(s)	
	Correlation Rules	
bwCallOverloadZoneTransition	Problem Type	Alarm
	OID	3618
	Status	current
	Severity Range	high
	Description	This trap is generated when the BroadWorks component enters a new non-call overload control zone.
	Problem Text	The server has entered a new call processing overload control zone. Old Zone: %npOldZone% New Zone: %npNewZone%
	Recommended Action(s)	
	Correlation Rules	
bwNonCallOverloadZoneTransition	Problem Type	Alarm
	OID	3619
	Status	current
	Severity Range	high
	Description	This trap is generated when the BroadWorks component enters a new call overload control zone.
	Problem Text	The server has entered a new non-call processing overload control zone. Old Zone: %npOldZone% New Zone: %npNewZone%
	Recommended Action(s)	
	Correlation Rules	
bwCongestionManagementNeighborOverloaded	Problem Type	Alarm
	OID	3635
	Status	current

Alarm Name	Attributes	Values
	Severity Range	medium
	Description	The Server has received a 503 Response with Retry-After from the neighbor and set the neighbor to Overloaded state.
	Problem Text	Neighbor: %npRemoteAddress% Retry-After period: %npPeriod%
	Recommended Action(s)	
	Correlation Rules	

8.2.9 SNMP Traps For Component: nssynch

The table that follows describes the SNMP traps for the nssynch subcomponent of the BroadworksFault MIB.

Table 22: SNMP Traps For BroadworksFault:nssynch

Alarm Name	Attributes	Values
bwNSSynchronizationConnectivityFailure	Problem Type	Notification
	OID	3537
	Status	current
	Severity Range	high
	Description	Failure to create data synchronization connection between Application Server and Network Server.
	Problem Text	Failure with connectivity between Application Server and Network Server for synchronization. %npReason%
	Recommended Action(s)	*
	Correlation Rules	
bwNSLocationConnectivityFailure	Problem Type	Alarm
	OID	3539
	Status	current
	Severity Range	high
	Description	Failure with connectivity between the Application Server and the Network Server.
	Problem Text	Failure with connectivity between Application Server and Network Server for user location. %npReason% Failed Transaction: %npMessage%
	Recommended Action(s)	*
	Correlation Rules	

Alarm Name	Attributes	Values
bwNSLocationFailure	Problem Type	Notification
	OID	3540
	Status	current
	Severity Range	medium
	Description	Data may be out of synch between the Application Server and the Network Server.
	Problem Text	Failure with user location transaction between Application Server and Network Server. %npReason% Failed Transaction: %npMessage% Network Server IP address: %npRemoteAddress%
	Recommended Action(s)	Check synchronization of data with Network Server used for user location.
	Correlation Rules	
bwNSSyncSuccessDbCommitFailed	Problem Type	Notification
	OID	11759
	Status	current
	Severity Range	medium
	Description	A provisioning transaction successfully performed a NSSynch but failed to commit to the database.
	Problem Text	Out of synch with NS : %npRequestName%
	Recommended Action(s)	
	Correlation Rules	

8.2.10 SNMP Traps For Component: smap

The table that follows describes the SNMP traps for the smap subcomponent of the BroadworksFault MIB.

Table 23: SNMP Traps For BroadworksFault:smap

Alarm Name	Attributes	Values
bwSMAPConnectionFailure	Problem Type	Notification
	OID	26
	Status	current
	Severity Range	medium
	Description	The SMAP port failed to be opened.
	Problem Text	Unable to open SMAP port, which will prevent processing of SNMP requests.

Alarm Name	Attributes	Values
	Recommended Action(s)	Stop server. Make sure SMAP port * is available for connection. Restart server. If problem persists, contact BroadSoft Support Engineer.
	Correlation Rules	

8.2.11 SNMP Traps For Component: accounting

The table that follows describes the SNMP traps for the accounting subcomponent of the BroadworksFault MIB.

Table 24: SNMP Traps For BroadworksFault:accounting

Alarm Name	Attributes	Values
bwLicenseMonitoringFault	Problem Type	Notification
	OID	3665
	Status	current
	Severity Range	high
	Description	Licensing threshold exceeded.
	Problem Text	bwLicenseMon has detected that some services have exceeded the following licensing threshold: %npCurrentThresholdValue% %npReport%
	Recommended Action(s)	
	Correlation Rules	

8.2.12 SNMP Traps For Component: licensing

The table that follows describes the SNMP traps for the licensing subcomponent of the BroadworksFault MIB.

Table 25: SNMP Traps For BroadworksFault:licensing

Alarm Name	Attributes	Values
bwLicenseFileNotFound	Problem Type	Notification
	OID	25
	Status	current
	Severity Range	critical
	Description	This notification indicates that the system is unable to locate the license files.
	Problem Text	License file not found. %npFilename%
	Recommended Action(s)	Install the license file or contact Broadsoft support.
	Correlation Rules	
bwLicenseFileExpiring	Problem Type	Notification
	OID	44
	Status	current

Alarm Name	Attributes	Values
	Severity Range	critical
	Description	This alarm is generated once a day when the license file expiration date is less than seven days from the current day.
	Problem Text	The license file will expire on %npDate%. After that date, the system will no longer start.
	Recommended Action(s)	Please contact BroadSoft to get an updated license file.
	Correlation Rules	
bwLicenseFileExpired	Problem Type	Notification
	OID	45
	Status	current
	Severity Range	critical
	Description	This alarm is sent once a day, after the license file has expired.
	Problem Text	The license file expired on %npDate%. The system can no longer start.
	Recommended Action(s)	Please contact BroadSoft to get an updated license file.
	Correlation Rules	
bwLicenseAuthenticationFailure	Problem Type	Notification
	OID	3541
	Status	current
	Severity Range	critical
	Description	This notification indicates that the authentication of the license file failed.
	Problem Text	License file authentication failure.
	Recommended Action(s)	Use the correct license file or contact Broadsoft support.
	Correlation Rules	
bwLicenseHWViolation	Problem Type	Notification
	OID	3543
	Status	current
	Severity Range	critical
	Description	This notification indicates that there is an attempt to run the application on an unlicensed server.
	Problem Text	Attempt to run the application on an unlicensed server.
	Recommended Action(s)	Please run the application on the designated server or contact BroadSoft to obtain additional licenses.
	Correlation Rules	
bwLicenseAccntViolation	Problem Type	Notification

Alarm Name	Attributes	Values
	OID	3544
	Status	current
	Severity Range	high
	Description	This notification indicates that the license allocation has exceeded the limit.
	Problem Text	License allocation has exceeded the limit for %npLicenseKey %. Limit is %npLicenseLimit% and current allocation is %npLicenseAllocation%.
	Recommended Action(s)	Please contact BroadSoft to obtain additional licenses.
	Correlation Rules	

8.2.13 SNMP Traps For Component: pmReporting

The table that follows describes the SNMP traps for the pmReporting subcomponent of the BroadworksFault MIB.

Table 26: SNMP Traps For BroadworksFault:pmReporting

Alarm Name	Attributes	Values
bwPMReportingFTPConnectionError	Problem Type	Alarm
	OID	16
	Status	current
	Severity Range	informational
	Description	Periodic measurement report could not be sent to FTP server.
	Problem Text	Periodic SNMP measurement report could not be sent to FTP server. Could not connect to %npRemoteAddress%. User ID: %npUserId%
	Recommended Action(s)	Verify the availability of the FTP server. Verify that the FTP domain, user ID and password are correct. The report file was copied to the /var/broadworks/pm_reports/not_sent directory. It can be uploaded manually to the FTP server.
	Correlation Rules	

8.2.14 SNMP Traps For Component: smdi

The table that follows describes the SNMP traps for the smdi subcomponent of the BroadworksFault MIB.

Table 27: SNMP Traps For BroadworksFault:smdi

Alarm Name	Attributes	Values
bwSMDIsessionRejected	Problem Type	Notification
	OID	3566
	Status	current
	Severity Range	low
	Description	An SMDI session, initiated by an external terminal server, was rejected.

Alarm Name	Attributes	Values
	Problem Text	An SMDI session was rejected. Rejection reason: %npReason%. Client address: %npClientAddress%.
	Recommended Action(s)	1- Make sure that the server sending the request is configured in the AS access list, 2- Try to increase to maximum number of sessions.
	Correlation Rules	
bwSMDIInterfaceError	Problem Type	Notification
	OID	3574
	Status	current
	Severity Range	low
	Description	The SMDI interface could not be started on a specific port.
	Problem Text	The SMDI interface cannot be enabled using listening port %npLocalPort%. The Application Server will not be able to receive or send SMDI messages.
	Recommended Action(s)	Validate whether: 1- The listening port specified is not already used by another application in the system. 2- The SMDI component is allowed to use the listening port specified. 3- Enabling the interface using another port works.
	Correlation Rules	
bwSMDIConfigurationError	Problem Type	Notification
	OID	3575
	Status	current
	Severity Range	low
	Description	An outgoing SMDI message could not be sent to a SMDI device for the specified user.
	Problem Text	The following user could not be mapped to an outgoing SMDI device: User ID: %npUserId% SMDI number: %npSmdiNumber%
	Recommended Action(s)	For Outgoing Message Waiting Indicator (MWI), verify that: 1- In Voice Messaging Service, Outgoing MWI is assigned and turned on for the user, 2- The SMDI route list is properly configured. For Message Desk (MD), verify that: 1- At least one outgoing SMDI device (terminal server) is configured for the SMDI Message Desk service.
	Correlation Rules	
bwSMDIOperationFailure	Problem Type	Notification

Alarm Name	Attributes	Values
	OID	3576
	Status	current
	Severity Range	low
	Description	For the actual description, refer the BroadWorks FaultManagementGuide as it may contain variable data.
	Problem Text	The SMDI MWI indicator was not accepted by the destination PBX or C5 network: User ID: %npUserId% SMDI number: %npSmdiNumber% Reason: %npReason%
	Recommended Action(s)	Validate whether: 1- The user should be assigned MWI on SMDI in the voice messaging service, or 2- The configuration on the PBX and/or class 5 is accurate.
	Correlation Rules	
bwSMDIRouteExhaustion	Problem Type	Notification
	OID	3577
	Status	current
	Severity Range	low
	Description	An SMDI message could not be sent because of route exhaustion.
	Problem Text	The SMDI MWI indicator cannot be sent to any SMDI device: User ID: %npUserId% SMDI number: %npSmdiNumber% Devices: %npDeviceName%
	Recommended Action(s)	Validate whether: 1- The SMDI device address and port are valid and reachable, or 2- The SMDI device configuration is accurate, or 3- The SMDI device is running and correctly communicating with the PBX and/or class 5.
	Correlation Rules	

8.2.15 SNMP Traps For Component: cpeDeviceManagement

The table that follows describes the SNMP traps for the cpeDeviceManagement subcomponent of the BroadworksFault MIB.

Table 28: SNMP Traps For BroadworksFault:cpeDeviceManagement

Alarm Name	Attributes	Values
bwCPEDeviceProfileLockout	Problem Type	Notification
	OID	66
	Status	current

Alarm Name	Attributes	Values
	Severity Range	low
	Description	Device Profile is locked out because of an authentication failure per device profile lockout rules.
	Problem Text	Device is locked out because of authentication failure. Service Provider / Enterprise ID: %npServiceProviderId% Group ID: %npGroupId% Device Profile Name: %npDeviceProfileName% Lockout Counter: %npLockoutCounter% Lockout Period (minutes): %npLockoutPeriod% %npDeviceFileRequestMessage%
	Recommended Action(s)	Determine if caused by a rogue device or configuration issue.
	Correlation Rules	

8.2.16 SNMP Traps For Component: networkDeviceManagement

The table that follows describes the SNMP traps for the networkDeviceManagement subcomponent of the BroadworksFault MIB.

Table 29: SNMP Traps For BroadworksFault:networkDeviceManagement

Alarm Name	Attributes	Values
bwNetworkDeviceIsFailed	Problem Type	Alarm
	OID	19
	Status	current
	Severity Range	high
	Description	This alarm is generated whenever a network device that was previously responding does not respond to an application-level ping.
	Problem Text	The following network device is currently unavailable: %npServerType% %npRemoteAddress%
	Recommended Action(s)	Please verify that the device is operational and that there is connectivity to the device.
	Correlation Rules	It is recommended to always keep the highest severity value for this notification until it is cleared.

8.2.17 SNMP Traps For Component: cap

The table that follows describes the SNMP traps for the cap subcomponent of the BroadworksFault MIB.

There is no visible fault for this component.

8.2.18 SNMP Traps For Component: ociReporting

The table that follows describes the SNMP traps for the ociReporting subcomponent of the BroadworksFault MIB.

Table 30: SNMP Traps For BroadworksFault:ociReporting

Alarm Name	Attributes	Values
bwOciReportingAclViolation	Problem Type	Notification
	OID	3607
	Status	current
	Severity Range	low
	Description	Connection request received from an unknown external system.
	Problem Text	External system IP address %npRemoteAddress% not in access control list.
	Recommended Action(s)	
	Correlation Rules	
bwOciReportingConnectionError	Problem Type	Alarm
	OID	3608
	Status	current
	Severity Range	low
	Description	Error detected on connection to an external system.
	Problem Text	Error detected on connection to external system IP address %npRemoteAddress%. Connection released.
	Recommended Action(s)	
	Correlation Rules	
bwOciReportingBackLogFileDeleted	Problem Type	Notification
	OID	3615
	Status	current
	Severity Range	low
	Description	The total size of the OCI reporting backlog files exceeded the system limit (500 MB). The oldest file is deleted.
	Problem Text	OCI Report backlog file %npFilename% for host %npHost% is deleted due to the system size limit.
	Recommended Action(s)	Reestablish the connection so the backlog files can be processed.
	Correlation Rules	

8.2.19 SNMP Traps For Component: bcct

The table that follows describes the SNMP traps for the bcct subcomponent of the BroadworksFault MIB.

Table 31: SNMP Traps For BroadworksFault:bcct

Alarm Name	Attributes	Values
bwCommProtocolInitError	Problem Type	Notification
	OID	28

Alarm Name	Attributes	Values
	Status	current
	Severity Range	high
	Description	Could not bind on TCP port.
	Problem Text	Application is unable to connect to local port: - Local Interface: %npLocalInterface% - Port: %npLocalPort%
	Recommended Action(s)	Make sure the listening port is not used by another application
	Correlation Rules	
bwCommProtocolHostNotAllowed	Problem Type	Notification
	OID	29
	Status	current
	Severity Range	low
	Description	A host that is not allowed for this protocol has attempted to connect.
	Problem Text	An unauthorized host for a specific protocol has attempted to connect to this server: - Remote Host Address: %npRemoteAddress% - Local Interface: %npLocalInterface% - Protocol: %npProtocol%
	Recommended Action(s)	In case of a valid host, make sure it is defined in the BCCT Access List for the specified protocol.
	Correlation Rules	
bwCommProtocolInterfaceNotAllowed	Problem Type	Notification
	OID	30
	Status	current
	Severity Range	low
	Description	Connections for this protocol are not allowed on this interface.
	Problem Text	A remote server has attempted to connect on an interface that is not registered for a protocol: - Remote Host Address: %npRemoteAddress% - Local Interface: %npLocalInterface% - Protocol: %npProtocol%
	Recommended Action(s)	In case of a valid host, make sure it is defined in the BCCT Access List for the specified protocol.
	Correlation Rules	

8.2.20 SNMP Traps For Component: taskMonitor

The table that follows describes the SNMP traps for the taskMonitor subcomponent of the BroadworksFault MIB.

Table 32: SNMP Traps For BroadworksFault:taskMonitor

Alarm Name	Attributes	Values
bwTaskMonitorWarning	Problem Type	Notification
	OID	34
	Status	current
	Severity Range	low
	Description	A task is taking longer than normal.
	Problem Text	A task is taking too long to complete. The task timeout is %npTimeLength% ms and it was started %npTimeElapsed% ms ago. Thread: %npThreadName%. Stack trace: %npStackTrace%
	Recommended Action(s)	Please report to BroadSoft support.
	Correlation Rules	
bwTaskMonitorHungTask	Problem Type	Notification
	OID	35
	Status	current
	Severity Range	high-critical
	Description	A task is hung.
	Problem Text	A task is hung. The task timeout is %npTimeLength% ms and it was started %npTimeElapsed% ms ago. Thread: %npThreadName% Stack trace: %npStackTrace%
	Recommended Action(s)	BroadWorks should be restarted as soon as possible. Please report to BroadSoft support.
	Correlation Rules	
bwTcpSubsystemFatalError	Problem Type	Notification
	OID	36
	Status	current
	Severity Range	high
	Description	TCP subsystem fatal error.
	Problem Text	TCP subsystem fatal error: shutdown initiated. %npStackTrace%
	Recommended Action(s)	Please report to BroadSoft support.
	Correlation Rules	

8.2.21 SNMP Traps For Component: logging

The table that follows describes the SNMP traps for the logging subcomponent of the BroadworksFault MIB.

Table 33: SNMP Traps For BroadworksFault:logging

Alarm Name	Attributes	Values
bwLogQueueSizeLimitReached	Problem Type	Alarm
	OID	42
	Status	current
	Severity Range	high
	Description	The server has started to drop log entries because the logging queue size limit has been reached.
	Problem Text	Log queue size reached %npSizeLimit% for the OutputChannels configured for %npFilename%
	Recommended Action(s)	Please verify the availability of the OutputChannels.
	Correlation Rules	

8.2.22 SNMP Traps For Component: dns

The table that follows describes the SNMP traps for the dns subcomponent of the BroadworksFault MIB.

Table 34: SNMP Traps For BroadworksFault:dns

Alarm Name	Attributes	Values
bwDnsTimeout	Problem Type	Notification
	OID	63
	Status	current
	Severity Range	high
	Description	A query to the Domain Name System (DNS) server times out.
	Problem Text	A DNS query timed out.
	Recommended Action(s)	
	Correlation Rules	
bwDnsServerUnreachable	Problem Type	Notification
	OID	3645
	Status	current
	Severity Range	low
	Description	A DNS server was unreachable for a DNS query.
	Problem Text	DNS server: %npRemoteAddress% is unreachable.
	Recommended Action(s)	
	Correlation Rules	
bwDnsAllServersUnreachable	Problem Type	Alarm
	OID	3646
	Status	current

Alarm Name	Attributes	Values
	Severity Range	high
	Description	All DNS servers are unreachable.
	Problem Text	All DNS servers are unreachable.
	Recommended Action(s)	
	Correlation Rules	

8.2.23 SNMP Traps For Component: snmpAgent

The table that follows describes the SNMP traps for the snmpAgent subcomponent of the BroadworksFault MIB.

Table 35: SNMP Traps For BroadworksFault:snmpAgent

Alarm Name	Attributes	Values
bwAlarmsTableLimitReached	Problem Type	Notification
	OID	47
	Status	current
	Severity Range	critical
	Description	This alarm is raised when the alarms table has reached the configured maximum number of entries. It warns the manager that no more alarms will be sent until the problem is fixed.
	Problem Text	The alarms table has reached its capacity limit of %npMaximumNbItems%. No more alarms will be sent until alarms are cleared.
	Recommended Action(s)	
	Correlation Rules	

8.2.24 SNMP Traps For Component: xsp

The table that follows describes the SNMP traps for the xsp subcomponent of the BroadworksFault MIB.

Table 36: SNMP Traps For BroadworksFault:xsp

Alarm Name	Attributes	Values
bwProtocolRegistrationFailure	Problem Type	Alarm
	OID	89
	Status	current
	Severity Range	high
	Description	Failed to register protocol with Application Server.
	Problem Text	
	Recommended Action(s)	
	Correlation Rules	
bwOCIPServerUnreachable	Problem Type	Alarm

Alarm Name	Attributes	Values
	OID	91
	Status	current
	Severity Range	high
	Description	Unable to send OCI-P request, server is unreachable.
	Problem Text	Unable to send OCI-P request to %npAddress%. Server is unreachable.
	Recommended Action(s)	Verify * connectivity
	Correlation Rules	
bwOCICServerUnreachable	Problem Type	Alarm
	OID	92
	Status	current
	Severity Range	high
	Description	Unable to send OCI-C request, server is unreachable.
	Problem Text	Unable to send OCI-C request to %npAddress%. Server is unreachable.
	Recommended Action(s)	Verify * connectivity.
	Correlation Rules	

8.2.25 SNMP Traps For Component: ps

The table that follows describes the SNMP traps for the ps subcomponent of the BroadworksFault MIB.

Table 37: SNMP Traps For BroadworksFault:ps

Alarm Name	Attributes	Values
bwSCFAPIURLUnreachable	Problem Type	Alarm
	OID	2607
	Status	current
	Severity Range	high
	Description	Connection to SCF API failed due to URL not being reachable.
	Problem Text	Could not connect to SCF API URL %npRemoteAddress%.
	Recommended Action(s)	
	Correlation Rules	

8.2.26 SNMP Traps For Component: softwareManager

The table that follows describes the SNMP traps for the softwareManager subcomponent of the BroadworksFault MIB.

Table 38: SNMP Traps For BroadworksFault:softwareManager

Alarm Name	Attributes	Values
bwMemoryAllocationExceeded	Problem Type	Notification
	OID	53
	Status	current
	Severity Range	informational
	Description	Reports a lack of memory when deploying an application..
	Problem Text	Total application memory usage (%npApplicationMemory% MB) exceeded system memory capacity (%npSystemMemory% MB).
	Recommended Action(s)	Please consider un-deploying some applications.
	Correlation Rules	
bwMemoryOverAllocation	Problem Type	Alarm
	OID	54
	Status	current
	Severity Range	informational
	Description	The memory allocation for application is overallocated.
	Problem Text	Memory settings for the containers on the node cannot be satisfied as configured. This condition is checked by the software manager on restart and when a new configuration is deployed on the node.
	Recommended Action(s)	The amount of memory configured for the containers exceeds the amount of physical memory.
	Correlation Rules	

8.2.27 SNMP Traps For Component: security

The table that follows describes the SNMP traps for the security subcomponent of the BroadworksFault MIB.

Table 39: SNMP Traps For BroadworksFault:security

Alarm Name	Attributes	Values
bwMaximumFailedLoginAttempts	Problem Type	Notification
	OID	27
	Status	current
	Severity Range	low
	Description	A user has failed to log in the allowed maximum number of times (consecutive login failures).
	Problem Text	The number of failed login attempts: %npFailedLoginAttempts% has exceeded the maximum of %npMaxFailedLoginAttempts%.
	Recommended Action(s)	
	Correlation Rules	

Alarm Name	Attributes	Values
bwMaximumFailedUserLoginAttempts	Problem Type	Notification
	OID	59
	Status	current
	Severity Range	low
	Description	A specific user/administrator has failed to log in the allowed maximum number of times (consecutive login failures).
	Problem Text	The user %npUserId% has reached the maximum number allowed (%npMaxFailedLoginAttempts%) of consecutive failed attempts, this account login has been disabled.
	Recommended Action(s)	
	Correlation Rules	
bwSecureTlktToolResult	Problem Type	Notification
	OID	64
	Status	current
	Severity Range	critical, high, medium, low, or informational
	Description	This notification returns the result from executing one of the Security Toolkit tool as a task where the tool is configured to report a notification.
	Problem Text	Result for tool %npSecureTlktToolName% Tool result: %npSecureTlktToolResult%
	Recommended Action(s)	
	Correlation Rules	
bwSecurityRiskDetected	Problem Type	Notification
	OID	68
	Status	current
	Severity Range	high
	Description	A security risk is detected.
	Problem Text	The Security Monitor maintenance task detects a security risk.
	Recommended Action(s)	Please review *.
	Correlation Rules	
bwKeyManagerCriticalDataMismatch	Problem Type	Notification
	OID	69
	Status	current
	Severity Range	high-critical
	Description	The key manager identified a mismatch between the password and the keystore entity.

Alarm Name	Attributes	Values
	Problem Text	Mismatch: the %npMissingComponent% is %npState% for the %npExistingComponent% that already exists.
	Recommended Action(s)	
	Correlation Rules	
bwChangeDatabaseUserPasswordError	Problem Type	Notification
	OID	70
	Status	current
	Severity Range	low
	Description	An error occurred while changing the password.
	Problem Text	An error occurred while changing the database password of %npUserName%. The previous password is still effective.
	Recommended Action(s)	Please ensure the database engine is running and retry with a different password.
	Correlation Rules	

8.2.28 SNMP Traps For Component: webcontainer

The table that follows describes the SNMP traps for the webcontainer subcomponent of the BroadworksFault MIB.

Table 40: SNMP Traps For BroadworksFault:webcontainer

Alarm Name	Attributes	Values
bwExecutorQueueUsageExceeded	Problem Type	Alarm
	OID	6005
	Status	current
	Severity Range	high
	Description	The usage ratio of the executor queue (in %) exceeded the threshold level.
	Problem Text	The usage ratio of the %npExecutorType% executor exceeded the threshold level.
	Recommended Action(s)	Review server usage for identifying potential bottlenecks.
	Correlation Rules	
bwExecutorQueueLatencyExceeded	Problem Type	Alarm
	OID	6006
	Status	current
	Severity Range	high
	Description	The executor queue latency exceeded the threshold level.
	Problem Text	The %npExecutorType% executor queue latency exceeded the threshold level.

Alarm Name	Attributes	Values
	Recommended Action(s)	Review server usage for identifying potential bottlenecks.
	Correlation Rules	
bwExecutorThreadPoolProcessingTime Exceeded	Problem Type	Alarm
	OID	6007
	Status	current
	Severity Range	high
	Description	The executor thread pool processing time exceeded the threshold level.
	Problem Text	The %npExecutorType% executor thread pool processing time exceeded the threshold level.
	Recommended Action(s)	Review server usage for identifying potential bottlenecks.
	Correlation Rules	
bwExecutorThreadPoolBusyExceeded	Problem Type	Alarm
	OID	6008
	Status	current
	Severity Range	high
	Description	The executor thread pool busy ratio exceeded the threshold level.
	Problem Text	The %npExecutorType% executor thread pool busy ratio exceeded the threshold level.
	Recommended Action(s)	Review server usage for identifying potential bottlenecks.
	Correlation Rules	

8.2.29 SNMP Traps For Component: sccp

The table that follows describes the SNMP traps for the sccp subcomponent of the BroadworksFault MIB.

There is no visible fault for this component.

8.2.30 SNMP Traps For Component: jvmProcess

The table that follows describes the SNMP traps for the jvmProcess subcomponent of the BroadworksFault MIB.

Table 41: SNMP Traps For BroadworksFault:jvmProcess

Alarm Name	Attributes	Values
bwHeapMemoryUsageExceeded	Problem Type	Alarm
	OID	61
	Status	current
	Severity Range	high
	Description	The memory usage ratio after a full garbage collection (in %) exceeded the threshold level.

Alarm Name	Attributes	Values
	Problem Text	The memory usage after a full garbage collection reached %npProcessMemoryUsage% M for %npContainerName%.
	Recommended Action(s)	Review server usage for identifying potential memory bottlenecks.
	Correlation Rules	
bwJVMProcessOutOfMemory	Problem Type	Alarm
	OID	74
	Status	current
	Severity Range	critical
	Description	An out of memory condition was detected by a thread.
	Problem Text	An out of memory condition has been detected by thread %npThreadName% for container %npContainerName%.
	Recommended Action(s)	Please contact BroadSoft support.
	Correlation Rules	
bwJVMProcessUnexpectedSoftwareConditionDetected	Problem Type	Alarm
	OID	75
	Status	current
	Severity Range	high
	Description	An unexpected software condition has been detected by a thread.
	Problem Text	An unexpected software condition has been detected by thread %npThreadName% for container %npContainerName%. Message: %npErrorMessage%
	Recommended Action(s)	Further details can be found in the container's output logs. Please contact BroadSoft support.
	Correlation Rules	
bwNonheapMemoryUsageExceeded	Problem Type	Alarm
	OID	62
	Status	deprecated
	Severity Range	high
	Description	The non heap memory usage ratio after a full garbage collection (in %) exceeded the threshold level.
	Problem Text	The non heap memory usage after a full garbage collection reached %npProcessMemoryUsage% M for %npContainerName%.
	Recommended Action(s)	Review server usage for identifying potential memory bottlenecks.
	Correlation Rules	

8.2.31 SNMP Traps For Component: time

The table that follows describes the SNMP traps for the time subcomponent of the BroadworksFault MIB.

Table 42: SNMP Traps For BroadworksFault:time

Alarm Name	Attributes	Values
bwTimeSkewExceeded	Problem Type	Notification
	OID	76
	Status	current
	Severity Range	medium
	Description	The time difference between servers exceeds threshold.
	Problem Text	The time difference with %npRemoteAddress% exceeds the %npTimeLength% seconds allowed threshold.
	Recommended Action(s)	Check the time on the servers. Check that NTP is correctly configured on the servers.
	Correlation Rules	

8.2.32 SNMP Traps For Component: webrtc

The table that follows describes the SNMP traps for the webrtc subcomponent of the BroadworksFault MIB.

There is no visible fault for this component.

8.2.33 SNMP Traps For Component: sipLocation

The table that follows describes the SNMP traps for the sipLocation subcomponent of the BroadworksFault MIB.

There is no visible fault for this component.

8.2.34 SNMP Traps For Component: threshold

The table that follows describes the SNMP traps for the threshold subcomponent of the BroadworksFault MIB.

Table 43: SNMP Traps For BroadworksFault:threshold

Alarm Name	Attributes	Values
bwCounterThreshold	Problem Type	Notification
	OID	13
	Status	current
	Severity Range	variable
	Description	Sent when a counter threshold reaches its limit.
	Problem Text	Counter %npCounterName% has reached or exceeded a user-defined threshold. The counter's value is %npCurrentCounterValue% and the threshold was set at %npCurrentThresholdValue%. The value to reach before the next notification is now %npNewThresholdValue%. User-defined description follows. %npThresholdDescription%

Alarm Name	Attributes	Values
	Recommended Action(s)	
	Correlation Rules	
bwGaugeLowLimitThreshold	Problem Type	Alarm
	OID	14
	Status	current
	Severity Range	variable
	Description	Sent when gauge threshold lowNotify value is reached while decreasing.
	Problem Text	Gauge %npGaugeName% has reached a user-defined low notification threshold. The threshold low value is %npCurrentThresholdValue% and the value to reach to clear the alarm is %npClearThresholdValue%. User-defined description follows. %npThresholdDescription%
	Recommended Action(s)	
	Correlation Rules	
bwGaugeHighLimitThreshold	Problem Type	Alarm
	OID	15
	Status	current
	Severity Range	variable
	Description	Sent when gauge threshold highNotify value is reached while increasing.
	Problem Text	Gauge %npGaugeName% has reached a user-defined high notification threshold. The threshold high value is %npCurrentThresholdValue% and the value to reach to clear the alarm is %npClearThresholdValue%. User-defined description follows. %npThresholdDescription%
	Recommended Action(s)	
	Correlation Rules	

8.2.35 SNMP Traps For Component: nps

The table that follows describes the SNMP traps for the nps subcomponent of the BroadworksFault MIB.

Table 44: SNMP Traps For BroadworksFault:nps

Alarm Name	Attributes	Values
bwPushNotificationServerUnreachable	Problem Type	Alarm
	OID	85
	Status	current
	Severity Range	critical

Alarm Name	Attributes	Values
	Description	Push Notification Server has become unreachable.
	Problem Text	Push Notification Server %npAddress% has become unreachable.
	Recommended Action(s)	Please verify Push Notification Server connectivity.
	Correlation Rules	

8.2.36 SNMP Traps For Component: hazelcastClient

The table that follows describes the SNMP traps for the hazelcastClient subcomponent of the BroadworksFault MIB.

Table 45: SNMP Traps For BroadworksFault:hazelcastClient

Alarm Name	Attributes	Values
bwHazelcastClusterConnectivity Unavailable	Problem Type	Alarm
	OID	86
	Status	current
	Severity Range	critical
	Description	The connectivity between Hazelcast client and Hazelcast cluster is unavailable.
	Problem Text	Connectivity to %npClusterName% is unavailable.
	Recommended Action(s)	Verify connectivity to Hazelcast cluster nodes or availability of Hazelcast cluster nodes.
	Correlation Rules	

8.3 BW-LicenseManagerFault MIB

This section presents SNMP traps (notifications and alarms) for the BW-LicenseManagerFault MIB grouped by component.

This MIB defines the faults for the BroadWorks license manager daemon.

Applicable server(s):

Network Server.

8.3.1 SNMP Traps For Component: processmonitor

The table that follows describes the SNMP traps for the processmonitor subcomponent of the BW-LicenseManagerFault MIB.

Table 46: SNMP Traps For BW-LicenseManagerFault:processmonitor

Alarm Name	Attributes	Values
bwPMlmdLaunched	Problem Type	Notification
	OID	15801
	Status	current
	Severity Range	informational

Alarm Name	Attributes	Values
	Description	This notification indicates that the license manager daemon has started.
	Problem Text	The license manager has started.
	Recommended Action(s)	
	Correlation Rules	bwPMlmdLaunched, bwPMlmdShutDown, bwPMlmdRestarted, and bwPMlmdDeath can be correlated into a single alarm. These events have to be considered as a transition of the state machine for the management of the LicenseController process
bwPMlmdShutDown	Problem Type	Notification
	OID	15802
	Status	current
	Severity Range	informational
	Description	This notification indicates that the license manager daemon has been manually shut down.
	Problem Text	The license manager has shutdown.
	Recommended Action(s)	
	Correlation Rules	bwPMlmdLaunched, bwPMlmdShutDown, bwPMlmdRestarted, and bwPMlmdDeath can be correlated into a single alarm. These events have to be considered as a transition of the state machine for the management of the LicenseController process
bwPMlmdRestarted	Problem Type	Notification
	OID	15803
	Status	current
	Severity Range	informational
	Description	This notification provides the date and time of the license manager daemon restart.
	Problem Text	The license manager has restarted.
	Recommended Action(s)	
	Correlation Rules	bwPMlmdLaunched, bwPMlmdShutDown, bwPMlmdRestarted, and bwPMlmdDeath can be correlated into a single alarm. These events have to be considered as a transition of the state machine for the management of the LicenseController process
bwPMlmdDeath	Problem Type	Notification
	OID	15804
	Status	current
	Severity Range	critical
	Description	This notification indicates that the license manager daemon has abnormally terminated.
	Problem Text	The License has terminated.

Alarm Name	Attributes	Values
	Recommended Action(s)	Ensure license manager is restarted.
	Correlation Rules	bwPMlmdLaunched, bwPMlmdShutDown, bwPMlmdRestarted, and bwPMlmdDeath can be correlated into a single alarm. These events have to be considered as a transition of the state machine for the management of the LicenseController process

8.3.2 SNMP Traps For Component: licensing

The table that follows describes the SNMP traps for the licensing subcomponent of the BW-LicenseManagerFault MIB.

Table 47: SNMP Traps For BW-LicenseManagerFault:licensing

Alarm Name	Attributes	Values
bwLicensingNFMCommunicationLoss	Problem Type	Alarm
	OID	15806
	Status	current
	Severity Range	high
	Description	There is a communication loss with the Network Function Manager.
	Problem Text	The license manager could not connect to Networks Function Manager at %npNFMFqdn%.
	Recommended Action(s)	Fix the connection between this node and the Network Function Manager.
	Correlation Rules	
bwLicensingLMCommunicationLoss	Problem Type	Alarm
	OID	15807
	Status	current
	Severity Range	high
	Description	There is a communication loss with the license manager.
	Problem Text	Unable to connect to the license manager.
	Recommended Action(s)	Ensure the license manager daemon is alive on this node.
	Correlation Rules	
bwLicensingViolation	Problem Type	Alarm
	OID	15808
	Status	current
	Severity Range	high
	Description	There is a license usage violation.
	Problem Text	This node is not allowed to use the current license, %npLicenseId%, %npBroadWorksRelease%, %npDate%.
	Recommended Action(s)	Please update the node with a valid license.

Alarm Name	Attributes	Values
	Correlation Rules	
bwLicensingOverAllocation	Problem Type	Alarm
	OID	15809
	Status	current
	Severity Range	high
	Description	An application reports a license over-allocation.
	Problem Text	An application reports a license over-allocation.
	Recommended Action(s)	Please update the license or de-provision the over-allocated application to clear the condition.
	Correlation Rules	
bwLicensingNFMCommunicationLossGrace	Problem Type	Notification
	OID	15810
	Status	current
	Severity Range	low to critical
	Description	There is a communication loss grace period.
	Problem Text	This node is in licensing communication loss grace period. %npGraceAction% will be executed in %npHours% hours.
	Recommended Action(s)	Fix the connection between this node and the Network Function Manager.
	Correlation Rules	
bwLicensingLMCommunicationLossGrace	Problem Type	Notification
	OID	15811
	Status	current
	Severity Range	low to critical
	Description	There is a communication loss grace period.
	Problem Text	This node is in licensing communication loss grace period. %npGraceAction% will be executed in %npHours% hours.
	Recommended Action(s)	Ensure the license manager daemon is alive on the machine.
	Correlation Rules	
bwLicensingViolationGrace	Problem Type	Notification
	OID	15812
	Status	current
	Severity Range	low to high
	Description	There is a licensing violation grace period.
	Problem Text	This node is in licensing violation grace period. %npGraceAction% will be executed in %npHours% hours.

Alarm Name	Attributes	Values
	Recommended Action(s)	Update the node with a valid license.
	Correlation Rules	
bwOverAllocationViolationGrace	Problem Type	Notification
	OID	15813
	Status	current
	Severity Range	low to high
	Description	There is a licensing over-allocation grace period.
	Problem Text	This node is in licensing over allocation grace period. %npGraceAction% will be executed in %npHours% hours.
	Recommended Action(s)	Update the license or de-provision the node to clear the over-allocation condition.
	Correlation Rules	

8.4 BW-NSExecutionFault MIB

This section presents SNMP traps (notifications and alarms) for the BW-NSExecutionFault MIB grouped by component.

This MIB defines the faults for the BroadWorks NS Execution application.

Applicable server(s):

Network Server.

8.4.1 SNMP Traps For Component: processmonitor

The table that follows describes the SNMP traps for the processmonitor subcomponent of the BW-NSExecutionFault MIB.

Table 48: SNMP Traps For BW-NSExecutionFault:processmonitor

Alarm Name	Attributes	Values
bwPMNSExecutionServerLaunched	Problem Type	Notification
	OID	1001
	Status	current
	Severity Range	informational
	Description	This notification indicates that the Network Server (NS) Execution Server has been started.
	Problem Text	NS Execution server started.
	Recommended Action(s)	

Alarm Name	Attributes	Values
	Correlation Rules	bwPMNSExecutionServerLaunched, bwPMNSExecutionServerShutDown, bwPMNSExecutionServerRestarted, bwPMNSExecutionServerDeath and bwPMNSExecutionServerOutOfMemory can be correlated into a single alarm. These events have to be considered as a transition of the state machine for the management of the Network Server Execution Server process.
bwPMNSExecutionServerShutDown	Problem Type	Notification
	OID	1002
	Status	current
	Severity Range	informational
	Description	This notification indicates that the Network Server (NS) Execution Server has been manually shut down.
	Problem Text	NS Execution server shut down.
	Recommended Action(s)	
	Correlation Rules	bwPMNSExecutionServerLaunched, bwPMNSExecutionServerShutDown, bwPMNSExecutionServerRestarted, bwPMNSExecutionServerDeath and bwPMNSExecutionServerOutOfMemory can be correlated into a single alarm. These events have to be considered as a transition of the state machine for the management of the Network Server Execution Server process.
bwPMNSExecutionServerRestarted	Problem Type	Notification
	OID	1003
	Status	current
	Severity Range	informational
	Description	This notification provides the date and time of the Network Server (NS) Execution Server restart.
	Problem Text	NS Execution server restarted.
	Recommended Action(s)	Log in BroadWorks.
	Correlation Rules	bwPMNSExecutionServerLaunched, bwPMNSExecutionServerShutDown, bwPMNSExecutionServerRestarted, bwPMNSExecutionServerDeath and bwPMNSExecutionServerOutOfMemory can be correlated into a single alarm. These events have to be considered as a transition of the state machine for the management of the Network Server Execution Server process.
bwPMNSExecutionServerDeath	Problem Type	Notification
	OID	1004
	Status	current
	Severity Range	critical
	Description	This notification provides the date and time of the Network Server (NS) Execution Server death.

Alarm Name	Attributes	Values
	Problem Text	NS Execution server terminated.
	Recommended Action(s)	Make sure the NS Execution server gets restarted
	Correlation Rules	bwPMNSExecutionServerLaunched, bwPMNSExecutionServerShutDown, bwPMNSExecutionServerRestarted, bwPMNSExecutionServerDeath and bwPMNSExecutionServerOutOfMemory can be correlated into a single alarm. These events have to be considered as a transition of the state machine for the management of the Network Server Execution Server process.
bwPMNSExecutionServerOutOfMemory	Problem Type	Notification
	OID	1043
	Status	current
	Severity Range	high
	Description	This notification provides the date and time when the Network Server (NS) Execution Server ran out of memory.
	Problem Text	NS Execution server ran out of memory.
	Recommended Action(s)	Make sure the NS Execution server gets restarted
	Correlation Rules	bwPMNSExecutionServerLaunched, bwPMNSExecutionServerShutDown, bwPMNSExecutionServerRestarted, bwPMNSExecutionServerDeath, and bwPMNSExecutionServerOutOfMemory can be correlated into a single alarm. These events have to be considered as a transition of the state machine for the management of the Network Server Execution Server process.

8.4.2 SNMP Traps For Component: database

The table that follows describes the SNMP traps for the database subcomponent of the BW-NSExecutionFault MIB.

Table 49: SNMP Traps For BW-NSExecutionFault:database

Alarm Name	Attributes	Values
bwNSDatabaseDataInconsistencyError	Problem Type	Notification
	OID	1012
	Status	current
	Severity Range	medium
	Description	This notification indicates that an inconsistency has been introduced in the database.
	Problem Text	New data was introduced through SQL statements which create data inconsistency: %npMessage%
	Recommended Action(s)	*
	Correlation Rules	
bwNSInvalidDialPlan	Problem Type	Notification

Alarm Name	Attributes	Values
	OID	1014
	Status	current
	Severity Range	medium
	Description	States that a dial plan contains an invalid entry.
	Problem Text	Invalid dial plan entry: %npMessage%
	Recommended Action(s)	*
	Correlation Rules	
bwNSSCRPInconsistentList	Problem Type	Notification
	OID	1015
	Status	current
	Severity Range	informational
	Description	One of the Service Center policy instances has an inconsistent service center routing list.
	Problem Text	The service center routing list contain non valid entry(ies), probably without defined result. Instance Name: %npInstanceName%
	Recommended Action(s)	Check the service center routing list of * for inconsistency
	Correlation Rules	

8.4.3 SNMP Traps For Component: sip

The table that follows describes the SNMP traps for the sip subcomponent of the BW-NSExecutionFault MIB.

Table 50: SNMP Traps For BW-NSExecutionFault:sip

Alarm Name	Attributes	Values
bwNSCallGotTreatment	Problem Type	Notification
	OID	1013
	Status	current
	Severity Range	informational
	Description	This notification indicates that the following call has not been completed and received a treatment.
	Problem Text	This call received a treatment: From : %npUserId% To : %npRequestUriUser% Call-id : %npCallId% Treatment : %npTreatment% SIP code : %npSipErrorCode%
	Recommended Action(s)	None

Alarm Name	Attributes	Values
	Correlation Rules	

8.4.4 SNMP Traps For Component: filesystem

The table that follows describes the SNMP traps for the filesystem subcomponent of the BW-NSExecutionFault MIB.

Table 51: SNMP Traps For BW-NSExecutionFault:filesystem

Alarm Name	Attributes	Values
bwNSPolicyDeploymentError	Problem Type	Notification
	OID	1011
	Status	current
	Severity Range	low
	Description	This notification states that the Network Server has problems deploying a policy.
	Problem Text	Policy deployment error. Details: %npExceptionMessage%
	Recommended Action(s)	
	Correlation Rules	

8.4.5 SNMP Traps For Component: callp

The table that follows describes the SNMP traps for the callp subcomponent of the BW-NSExecutionFault MIB.

Table 52: SNMP Traps For BW-NSExecutionFault:callp

Alarm Name	Attributes	Values
bwNSMemLeakInSessionFactory	Problem Type	Notification
	OID	1010
	Status	current
	Severity Range	critical
	Description	This notification indicates that the internal session factory leaks. This could reduce the amount of memory available to the Network Server.
	Problem Text	Memory leak in session factory
	Recommended Action(s)	
	Correlation Rules	
bwNSASCapacityExceeded	Problem Type	Notification
	OID	1041
	Status	current
	Severity Range	critical
	Description	Too many users are provisioned against an Application Server set. This may cause overload and loss of service.

Alarm Name	Attributes	Values
	Problem Text	The Network Server can no longer safely assign users to Application Server set: %npApplicationServerSetName%. The number of users to be hosted by the Application Server set exceeds the total capacity of the set. The Application Server set currently contains the following Hosting NEs: %npApplicationServerSetContent%. This may cause overload conditions and loss of service.
	Recommended Action(s)	To resolve, perform one or more of the following actions: - Add one or more Hosting NEs to the set; - Increase the capacity of one or more Hosting NEs; - Assign one or more enterprises to another Application Server set; - Assign one or more groups to another Application Server set.
	Correlation Rules	
bwSubscriberXSPartitionMismatch	Problem Type	Notification
	OID	1042
	Status	current
	Severity Range	critical
	Description	Execution Server hosting subscriber is not in subscriber's NE maintenance partition.
	Problem Text	The Network Server moved a subscriber to an Execution Server which is not in the subscriber's NE maintenance partition. Service provider id: %npServiceProviderId% Group id: %npGroupId% Subscriber NE maintenance partition id: %npNEMaintenancePartitionId% AS set name: %npApplicationServerSetName%
	Recommended Action(s)	Make sure the subscriber's AS set has at least one Execution Server in the NE maintenance partition associated with the subscriber's subscriber maintenance partition.
	Correlation Rules	
bwLocalXSBlacklisted	Problem Type	Alarm
	OID	1044
	Status	current
	Severity Range	medium
	Description	An Execution Server address from the local data center is blacklisted. An Execution Server address is blacklisted when it fails to successfully process requests a configurable consecutive number of times. The alarm is cleared when the local Execution Server is back online following one or more successful response(s) to SIP OPTIONS requests.
	Problem Text	Execution Server address in local data center: %npRemoteAddress%. Name of the local data center: %npDataCenter%
	Recommended Action(s)	
	Correlation Rules	
bwRemoteXSBlacklisted	Problem Type	Alarm

Alarm Name	Attributes	Values
	OID	1045
	Status	current
	Severity Range	low
	Description	An Execution Server address from another data center is blacklisted. An Execution Server address is blacklisted when it fails to successfully process requests a configurable consecutive number of times. The alarm is cleared when the remote Execution Server is back online following one or more successful response(s) to SIP OPTIONS requests.
	Problem Text	Execution Server address in another data center: %npRemoteAddress%. Name of the remote data center: %npDataCenter%
	Recommended Action(s)	
	Correlation Rules	
bwNSBlacklisted	Problem Type	Alarm
	OID	1046
	Status	current
	Severity Range	high
	Description	The Network Server has blacklisted itself for XS Location request processing. This happens when the number of online Execution Servers from the local data center falls below a configurable threshold. The alarm is cleared when enough Execution Servers are back online.
	Problem Text	The Network Server has blacklisted itself for XS Location request processing.
	Recommended Action(s)	
	Correlation Rules	
bwNSCallPTimingVerificationToolFailure	Problem Type	Notification
	OID	1047
	Status	current
	Severity Range	medium
	Description	Something went wrong while executing the CallPTimingVerification tool and the test-suite has not been fully processed.
	Problem Text	Something went wrong while executing the CallPTimingVerification tool and the test-suite has not been fully processed.
	Recommended Action(s)	Please consult the callPTimingVerification tool error logs located under /var/broadworks/verif/log
	Correlation Rules	
bwNSCallPTimingVerificationThreshold Exceeded	Problem Type	Notification
	OID	1048

Alarm Name	Attributes	Values
	Status	current
	Severity Range	low-critical
	Description	Configured maximum query duration exceeded.
	Problem Text	Configured maximum query duration exceeded : Command : %npCommand% QueryDuration : %npQueryDuration% ConfiguredMax : %npConfiguredMax%
	Recommended Action(s)	Please consult the callPTimingVerification tool logs located under /var/broadworks/verif/log
	Correlation Rules	
bwNsCallPTimingVerificationQuery Degradation	Problem Type	Notification
	OID	1049
	Status	current
	Severity Range	low-critical
	Description	CallPTimingVerification tool detected query degradation.
	Problem Text	
	Recommended Action(s)	
	Correlation Rules	

8.4.6 SNMP Traps For Component: loggingserver

The table that follows describes the SNMP traps for the loggingserver subcomponent of the BW-NSExecutionFault MIB.

Table 53: SNMP Traps For BW-NSExecutionFault:loggingserver

Alarm Name	Attributes	Values
bwCallLogRegister	Problem Type	Notification
	OID	1019
	Status	current
	Severity Range	informational
	Description	Send when a client (that is, the CLI) registers with the call log server.
	Problem Text	Client %npRemoteAddress% registered with CallLogServer
	Recommended Action(s)	None
	Correlation Rules	
bwCallLogUnregister	Problem Type	Notification
	OID	1020
	Status	current
	Severity Range	informational

Alarm Name	Attributes	Values
	Description	Send when a client (that is, the CLI) un-registers from the call log server.
	Problem Text	Client %npRemoteAddress% un-registered from CallLogServer
	Recommended Action(s)	None
	Correlation Rules	
bwCallLogFailure	Problem Type	Notification
	OID	1021
	Status	current
	Severity Range	medium
	Description	Send when the server is unable to deliver a log to a given client.
	Problem Text	CallLogServer failed to send log to client %npRemoteAddress%
	Recommended Action(s)	Verify status of client
	Correlation Rules	
bwCallLogUnregisterFailure	Problem Type	Notification
	OID	1022
	Status	current
	Severity Range	informational
	Description	Send when the server un-registers an unreachable client.
	Problem Text	CallLogServer unregistered client %npRemoteAddress% because of too many communication failure
	Recommended Action(s)	Verify status of client
	Correlation Rules	

8.4.7 SNMP Traps For Component: nrs

The table that follows describes the SNMP traps for the nrs subcomponent of the BW-NSExecutionFault MIB.

Table 54: SNMP Traps For BW-NSExecutionFault:nrs

Alarm Name	Attributes	Values
bwNSASRUnknownHostError	Problem Type	Alarm
	OID	1023
	Status	current
	Severity Range	medium
	Description	The Network Server does not know about the hosting NE specified in the ASR request. The request cannot be processed.
	Problem Text	Unknown host (%npRemoteAddress%) specified in ASR MigrateRequest Event

Alarm Name	Attributes	Values
	Recommended Action(s)	Make sure that HOSTID specified in ASR messages matches a provisioned HostingNE
	Correlation Rules	

8.4.8 SNMP Traps For Component: licensing

The table that follows describes the SNMP traps for the licensing subcomponent of the BW-NSExecutionFault MIB.

Table 55: SNMP Traps For BW-NSExecutionFault:licensing

Alarm Name	Attributes	Values
bwNSUnlicensedFeature	Problem Type	Notification
	OID	1016
	Status	current
	Severity Range	medium
	Description	This alarm is sent when the Network Server loads a policy instance from a policy not correctly licensed.
	Problem Text	UnlicensedFeature %npPolicyFeature%
	Recommended Action(s)	Obtain or install appropriate license file
	Correlation Rules	
bwLicenseViolation	Problem Type	Notification
	OID	1034
	Status	current
	Severity Range	major
	Description	License violation. This alarm occurs when the number of transactions recorded in any time period exceeds the licensed maximum.
	Problem Text	License Violation: Exceeded the number of transaction licensed (%npNbTransactions% transactions) per Time Period (%npPeriod% secs).
	Recommended Action(s)	Contact BroadSoft to purchase additional licenses.
	Correlation Rules	
bwLicenseThreshold	Problem Type	Notification
	OID	1035
	Status	current
	Severity Range	high
	Description	This notification indicates that the system call processing traffic (transaction/sec) has reached 80% of the limit defined in the license file.

Alarm Name	Attributes	Values
	Problem Text	License Warning: Close to exceeding the number of transactions licensed (%npNbTransactions% transactions) per Time Period (%npPeriod% secs). Server now at %npCurrentThresholdValue%% of licensed capacity. (Keep in mind that redundant server does not count. For instance, a two-NS cluster at 40% _server_ capacity is in fact at 80% _cluster_ capacity. Please consult BroadWorks documentation.)
	Recommended Action(s)	Contact BroadSoft to purchase additional licenses.
	Correlation Rules	
bwNonInviteLicenseViolation	Problem Type	Notification
	OID	1038
	Status	current
	Severity Range	major
	Description	License violation. This alarm occurs when the number of non-SIP invite transactions recorded in any time period exceeds the licensed maximum.
	Problem Text	License Violation: Exceeded the number of non SIP invite transactions licensed (%npNbTransactions% transactions) per time period (%npPeriod% time period)
	Recommended Action(s)	Contact BroadSoft to purchase additional licenses.
	Correlation Rules	
bwNonInviteLicenseThreshold	Problem Type	Notification
	OID	1039
	Status	current
	Severity Range	major
	Description	This notification indicates that the system non-call processing traffic (non-SIP invite transaction/sec) has reached 80% of the limit defined in the license file.
	Problem Text	License Warning: Close to exceeding the number of non SIP invite transactions licensed (%npNbTransactions% transactions) per Time Period (%npPeriod% secs). Server now at %npCurrentThresholdValue%% of licensed capacity. (Keep in mind that redundant server does not count. For instance, a two-NS cluster at 40% _server_ capacity is in fact at 80% _cluster_ capacity. Please consult BroadWorks documentation.)
	Recommended Action(s)	Contact BroadSoft to purchase additional licenses.
	Correlation Rules	

8.4.9 SNMP Traps For Component: networkDeviceManagement

The table that follows describes the SNMP traps for the networkDeviceManagement subcomponent of the BW-NSExecutionFault MIB.

Table 56: SNMP Traps For BW-NSExecutionFault:networkDeviceManagement

Alarm Name	Attributes	Values
bwNetworkDeviceNodeIsFailed	Problem Type	Alarm
	OID	1032
	Status	current
	Severity Range	high
	Description	This alarm is generated whenever a network device node that was previously responding does not respond to an application-level ping.
	Problem Text	The following network device node is currently unavailable: %npDeviceType% %npDeviceName% Node: %npNodeId%
	Recommended Action(s)	Please verify that the device node is operational and that there is connectivity to the device node.
	Correlation Rules	

8.5 BW-NSPortalFault MIB

This section presents SNMP traps (notifications and alarms) for the BW-NSPortalFault MIB grouped by component.

This MIB defines the faults for the BroadWorks NS Portal application.

Applicable server(s):

Network Server.

8.5.1 SNMP Traps For Component: unspecified

The table that follows describes the SNMP traps for the unspecified subcomponent of the BW-NSPortalFault MIB.

Table 57: SNMP Traps For BW-NSPortalFault:unspecified

Alarm Name	Attributes	Values
bwServiceControlProxyConnFailed	Problem Type	Alarm
	OID	1036
	Status	current
	Severity Range	informational
	Description	The service control proxy experienced communication problems with a specific Application Server.
	Problem Text	This notification indicates the Service Control Proxy failed to make CAP connection to the Application Server. The Service Control Proxy failed to open a channel to Application Server %npRemoteAddress%.
	Recommended Action(s)	Make sure the Application Server can be reached using the specified IP address and port.
	Correlation Rules	
bwServiceControlProxyConnTerminated	Problem Type	Notification

Alarm Name	Attributes	Values
	OID	1037
	Status	current
	Severity Range	informational
	Description	This notification indicates a CAP connection between the service control proxy and the Application Server has been terminated.
	Problem Text	This notification indicates a CAP connection between the Service Control Proxy and the Application Server has been terminated. A connection has been terminated between the Service Control Proxy and the Application Server %npRemoteAddress%.
	Recommended Action(s)	Make sure the Application Server can be reached using the specified IP address and port.
	Correlation Rules	

8.5.2 SNMP Traps For Component: nslocation

The table that follows describes the SNMP traps for the nslocation subcomponent of the BW-NSPortalFault MIB.

Table 58: SNMP Traps For BW-NSPortalFault:nslocation

Alarm Name	Attributes	Values
bwLocationAPIRequestError	Problem Type	Notification
	OID	1040
	Status	current
	Severity Range	high
	Description	An error occurred while processing a location API request.
	Problem Text	An error occurred while processing a location API request.
	Recommended Action(s)	
	Correlation Rules	

8.5.3 SNMP Traps For Component: networkDeviceManagement

The table that follows describes the SNMP traps for the networkDeviceManagement subcomponent of the BW-NSPortalFault MIB.

Table 59: SNMP Traps For BW-NSPortalFault:networkDeviceManagement

Alarm Name	Attributes	Values
bwSCPNetworkDeviceNodeIsFailed	Problem Type	Alarm
	OID	1251
	Status	current
	Severity Range	high
	Description	This alarm is generated whenever a network device node that was previously responding does not respond to an application-level ping.

Alarm Name	Attributes	Values
	Problem Text	The following network device node is currently unavailable: %npDeviceType% %npDeviceName% Node: %npNodeId%
	Recommended Action(s)	Please verify that the device node is operational and that there is connectivity to the device node.
	Correlation Rules	

8.6 BW-NSProvisioningFault MIB

This section presents SNMP traps (notifications and alarms) for the BW-NSProvisioningFault MIB grouped by component.

This MIB defines the faults for the BroadWorks NS Provisioning application.

Applicable server(s):

Network Server.

8.6.1 SNMP Traps For Component: processmonitor

The table that follows describes the SNMP traps for the processmonitor subcomponent of the BW-NSProvisioningFault MIB.

Table 60: SNMP Traps For BW-NSProvisioningFault:processmonitor

Alarm Name	Attributes	Values
bwPMNSProvisioningServerLaunched	Problem Type	Notification
	OID	1005
	Status	current
	Severity Range	informational
	Description	This notification indicates that the Network Server (NS) Provisioning Server has been started.
	Problem Text	NS Provisioning server started.
	Recommended Action(s)	
	Correlation Rules	bwPMNSProvisioningServerLaunched, bwPMNSProvisioningServerShutDown, bwPMNSProvisioningServerRestarted, bwPMNSProvisioningServerDeath and bwPMNSProvisioningServerOutOfMemory can be correlated into a single alarm. These events have to be considered as a transition of the state machine for the management of the Network Server Provisioning Server process.
bwPMNSProvisioningServerShutDown	Problem Type	Notification
	OID	1006
	Status	current
	Severity Range	informational
	Description	This notification indicates that the Network Server (NS) Provisioning Server has been manually shut down.
	Problem Text	NS Provisioning server shut down.

Alarm Name	Attributes	Values
	Recommended Action(s)	
	Correlation Rules	bwPMNSProvisioningServerLaunched, bwPMNSProvisioningServerShutDown, bwPMNSProvisioningServerRestarted, bwPMNSProvisioningServerDeath and bwPMNSProvisioningServerOutOfMemory can be correlated into a single alarm. These events have to be considered as a transition of the state machine for the management of the Network Server Provisioning Server process.
bwPMNSProvisioningServerRestarted	Problem Type	Notification
	OID	1007
	Status	current
	Severity Range	informational
	Description	This notification provides the date and time of the Network Server (NS) Provisioning Server restart.
	Problem Text	NS Provisioning server restarted.
	Recommended Action(s)	Log in BroadWorks.
	Correlation Rules	bwPMNSProvisioningServerLaunched, bwPMNSProvisioningServerShutDown, bwPMNSProvisioningServerRestarted, bwPMNSProvisioningServerDeath and bwPMNSProvisioningServerOutOfMemory can be correlated into a single alarm. These events have to be considered as a transition of the state machine for the management of the Network Server Provisioning Server process.
bwPMNSProvisioningServerDeath	Problem Type	Notification
	OID	1008
	Status	current
	Severity Range	critical
	Description	This notification provides the date and time of the Network Server (NS) Provisioning Server death.
	Problem Text	NS Provisioning server terminated.
	Recommended Action(s)	Make sure the NS provisioning server gets restarted
	Correlation Rules	bwPMNSProvisioningServerLaunched, bwPMNSProvisioningServerShutDown, bwPMNSProvisioningServerRestarted, bwPMNSProvisioningServerDeath and bwPMNSProvisioningServerOutOfMemory can be correlated into a single alarm. These events have to be considered as a transition of the state machine for the management of the Network Server Provisioning Server process.
bwPMNSProvisioningServerOutOf Memory	Problem Type	Notification
	OID	1305
	Status	current
	Severity Range	high

Alarm Name	Attributes	Values
	Description	This notification provides the date and time when the Network Server (NS) Provisioning Server ran out of memory.
	Problem Text	NS Provisioning server ran out of memory.
	Recommended Action(s)	Make sure the NS Provisioning server gets restarted
	Correlation Rules	bwPMNSProvisioningServerLaunched, bwPMNSProvisioningServerShutDown, bwPMNSProvisioningServerRestarted, bwPMNSProvisioningServerDeath, and bwPMNSProvisioningServerOutOfMemory can be correlated into a single alarm. These events have to be considered as a transition of the state machine for the management of the Network Server Provisioning Server process.

8.6.2 SNMP Traps For Component: database

The table that follows describes the SNMP traps for the database subcomponent of the BW-NSProvisioningFault MIB.

Table 61: SNMP Traps For BW-NSProvisioningFault:database

Alarm Name	Attributes	Values
bwNSPSDatabaseDataInconsistencyError	Problem Type	Notification
	OID	1302
	Status	current
	Severity Range	medium
	Description	This notification indicates that an inconsistency has been introduced in the database.
	Problem Text	New data was introduced through SQL statements which create data inconsistency: %npMessage%
	Recommended Action(s)	*
	Correlation Rules	
bwNSPSInvalidDialPlan	Problem Type	Notification
	OID	1303
	Status	current
	Severity Range	medium
	Description	States that a dial plan contains an invalid entry.
	Problem Text	Invalid dial plan entry: %npMessage%
	Recommended Action(s)	*
	Correlation Rules	
bwNSPSSCRPInconsistentList	Problem Type	Notification
	OID	1304
	Status	current

Alarm Name	Attributes	Values
	Severity Range	informational
	Description	One of the Service Center policy instances has an inconsistent service center routing list.
	Problem Text	The service center routing list contain non valid entry(ies), probably without defined result. Instance Name: %npInstanceName%
	Recommended Action(s)	Check the service center routing list of * for inconsistency
	Correlation Rules	

8.6.3 SNMP Traps For Component: filesystem

The table that follows describes the SNMP traps for the filesystem subcomponent of the BW-NSProvisioningFault MIB.

Table 62: SNMP Traps For BW-NSProvisioningFault:filesystem

Alarm Name	Attributes	Values
bwNSPSPolicyDeploymentError	Problem Type	Notification
	OID	1301
	Status	current
	Severity Range	low
	Description	This notification states that the Network Server has problems deploying a policy.
	Problem Text	Policy deployment error. Details: %npExceptionMessage%
	Recommended Action(s)	
	Correlation Rules	

8.6.4 SNMP Traps For Component: nssynch

The table that follows describes the SNMP traps for the nssynch subcomponent of the BW-NSProvisioningFault MIB.

Table 63: SNMP Traps For BW-NSProvisioningFault:nssynch

Alarm Name	Attributes	Values
bwNSSynchUnknownHostnameError	Problem Type	Alarm
	OID	1024
	Status	current
	Severity Range	medium
	Description	This alarm is sent when a Network Server synchronization event is received from an unknown host.
	Problem Text	Unknown hostname for AS: %npRemoteAddress%
	Recommended Action(s)	*

Alarm Name	Attributes	Values
	Correlation Rules	
bwNSSynchTrustedKeyError	Problem Type	Notification
	OID	1025
	Status	current
	Severity Range	medium
	Description	This alarm is sent when a Network Server Synch event is received from host with an invalid sync key.
	Problem Text	Incorrect trusted key received from AS with hostname: %npRemoteAddress%
	Recommended Action(s)	*
	Correlation Rules	
bwNSSynchExceptionError	Problem Type	Notification
	OID	1026
	Status	current
	Severity Range	medium
	Description	This alarm is sent when an internal error is generated while processing a sync request.
	Problem Text	Cannot open a synchAPI session with AS with hostname: %npRemoteAddress% because of an exception. Stack Trace: %npStackTrace%
	Recommended Action(s)	Contact BroadSoft Support Engineer.
	Correlation Rules	
bwNSSynchUpdateXMLError	Problem Type	Notification
	OID	1027
	Status	current
	Severity Range	medium
	Description	This alarm is sent when a request from a given device cannot be processed by the Network Server sync API.
	Problem Text	Cannot perform synch update requested by Hosting NE: %npRemoteAddress%. Reason: %npReason% XML Request: %npRequest%
	Recommended Action(s)	Contact BroadSoft Support Engineer.
	Correlation Rules	
bwNSSynchUpdateFailureError	Problem Type	Notification

Alarm Name	Attributes	Values
	OID	1028
	Status	current
	Severity Range	medium
	Description	This alarm is sent when a request from a given device cannot be processed by the Network Server sync API.
	Problem Text	Cannot perform synch update requested by Hosting NE: %npRemoteAddress%. Reason: %npReason% Request Data: %npRequest%
	Recommended Action(s)	Verify the validity and consistency of related data on the AS and NS, and then manually update the NS with the request data. This condition can occur when the synch API was not properly configured initially upon installing the AS and NS.
	Correlation Rules	
bwNSSynchUpdateExceptionError	Problem Type	Notification
	OID	1029
	Status	current
	Severity Range	medium
	Description	This alarm is sent when a request from a given device cannot be processed by the Network Server sync API because of an internal software error.
	Problem Text	Cannot perform synch update requested by Hosting NE: %npRemoteAddress% because of a software error. Details: %npMessage% XML Request: %npRequest%
	Recommended Action(s)	Contact BroadSoft Support Engineer.
	Correlation Rules	
bwNSSynchUpdateIncorrectVersionError	Problem Type	Notification
	OID	1030
	Status	current
	Severity Range	medium
	Description	This alarm is sent when a request is received with an unknown version of the sync API protocol.
	Problem Text	Cannot perform synch update requested by Hosting NE: %npRemoteAddress%. The synch API version in the XML message is incorrect. Expecting: 1.0 or 2.0. Received: %npReceivedVersion%
	Recommended Action(s)	Contact BroadSoft Support Engineer.

Alarm Name	Attributes	Values
	Correlation Rules	
bwNSSynchUpdateIncorrectProtocolError	Problem Type	Notification
	OID	1031
	Status	current
	Severity Range	medium
	Description	This alarm is sent when a request is received with an unknown version of the sync API protocol.
	Problem Text	Cannot perform synch update requested by Hosting NE: %npRemoteAddress%. The synch API protocol in the XML message is incorrect. Expecting: %npExpectedVersion%. Received: %npReceivedVersion%
	Recommended Action(s)	Contact BroadSoft Support Engineer.
	Correlation Rules	

8.6.5 SNMP Traps For Component: nsClusterUpgrade

The table that follows describes the SNMP traps for the nsClusterUpgrade subcomponent of the BW-NSProvisioningFault MIB.

Table 64: SNMP Traps For BW-NSProvisioningFault:nsClusterUpgrade

Alarm Name	Attributes	Values
bwInterClusterConnectionFailure	Problem Type	Alarm
	OID	1306
	Status	current
	Severity Range	high
	Description	The connection with the remote Network Server cluster is down.
	Problem Text	The connection type %npConnectionType% with the remote Network Server cluster (%npRemoteAddresses%) is down.
	Recommended Action(s)	Verify that the remote cluster Network Server addresses are correctly provisioned and that the servers are running.
	Correlation Rules	

8.7 BW-WebContainerFault MIB

This section presents SNMP traps (notifications and alarms) for the BW-WebContainerFault MIB grouped by component.

This MIB defines the faults for the Web Container application.

Applicable server(s):

Network Server.

8.7.1 SNMP Traps For Component: webcontainer

The table that follows describes the SNMP traps for the webcontainer subcomponent of the BW-WebContainerFault MIB.

Table 65: SNMP Traps For BW-WebContainerFault:webcontainer

Alarm Name	Attributes	Values
bwWebContainerTransactionGlobalRate LimitExceeded	Problem Type	Notification
	OID	6001
	Status	current
	Severity Range	high
	Description	Transaction denial due to high transaction rate for a given webapp.
	Problem Text	Transaction denied due to high transaction rate for webapp %npWebAppContext%
	Recommended Action(s)	
	Correlation Rules	
bwWebContainerTransactionUserRate LimitExceeded	Problem Type	Notification
	OID	6002
	Status	current
	Severity Range	high
	Description	Transaction denial due to high transaction rate for a given userid.
	Problem Text	Transaction denied due to high transaction rate for webapp %npWebAppContext% and userid %npUserId%
	Recommended Action(s)	
	Correlation Rules	
bwWebApplicationCacheDiskFull	Problem Type	Alarm
	OID	6003
	Status	current
	Severity Range	low
	Description	A cache update has failed because the disk is full.
	Problem Text	The web application "%npWebAppName%" cache is out of space.
	Recommended Action(s)	Clean disk space or reduce the cache size on disk.
	Correlation Rules	
bwHttpWorkersBusyExceeded	Problem Type	Alarm
	OID	6004
	Status	current
	Severity Range	high
	Description	The ratio of http workerBusy exceeded the threshold level.
	Problem Text	The ratio of http workerBusy exceeded the threshold level.

Alarm Name	Attributes	Values
	Recommended Action(s)	Review server usage for identifying potential bottlenecks.
	Correlation Rules	
bwWebContainerServerTransactionLimit Exceeded	Problem Type	Notification
	OID	6009
	Status	current
	Severity Range	high
	Description	The number of incoming requests exceeded the prescribed limit during the last overload protection period.
	Problem Text	The number of incoming requests reached %npReceivedRequestsDuringLastPeriod% for the last %npProtectionPeriod% %npPeriodUnit%.
	Recommended Action(s)	Review incoming traffic to identify potential Denial of Service (DOS) attacks.
	Correlation Rules	
bwWebContainerWebAppTransaction LimitExceeded	Problem Type	Notification
	OID	6010
	Status	current
	Severity Range	high
	Description	The number of incoming requests exceeded the prescribed limit during the last overload protection period.
	Problem Text	The number of incoming requests for %npWebAppContext% reached %npReceivedRequestsDuringLastPeriod% for the last %npProtectionPeriod% %npPeriodUnit%.
	Recommended Action(s)	Review incoming traffic to identify potential Denial of Service (DOS) attacks.
	Correlation Rules	
bwWebContainerUserTransactionLimit Exceeded	Problem Type	Notification
	OID	6011
	Status	current
	Severity Range	high
	Description	The number of incoming requests exceeded the prescribed limit during the last overload protection period.
	Problem Text	The number of incoming requests from %npWebAppUser% for %npWebAppContext% reached %npReceivedRequestsDuringLastPeriod% for the last %npProtectionPeriod% %npPeriodUnit%.
	Recommended Action(s)	Review incoming traffic to identify potential Denial of Service (DOS) attacks.
	Correlation Rules	
bwWebContainerAuthenticationServer Unreachable	Problem Type	Alarm
	OID	6012

Alarm Name	Attributes	Values
	Status	current
	Severity Range	critical
	Description	The Web Container was unable to connect to the Authentication Server.
	Problem Text	The Web Container was unable to connect to the Authentication Server %npAuthenticationServer%.
	Recommended Action(s)	Identify why the WebContainer cannot communicate with the authentication server.
	Correlation Rules	
bwSslClientAuthWithoutTrust	Problem Type	Notification
	OID	6013
	Status	current
	Severity Range	high
	Description	There is no trust configured on the system but a client authentication is required on a secure interface.
	Problem Text	The client authentication is required on the %npProtocol% secure interface %npName% without any trust configured.
	Recommended Action(s)	Configure at least one valid trust anchor.
	Correlation Rules	

Appendix A: Additional Information

This section captures additional information related to Cisco BroadWorks Fault and Alarm Management.

9.1 Fault Parameters

This section captures the list of parameters that can are used by the various Cisco BroadWorks faults.

Table 66: Fault Parameters

Parameter Name	Attributes	Values
npAlarmList	OID	1
	Description	Describes a list of alarms
	Type	DisplayString
npAllowedAttempts	OID	2
	Description	The number of allowed attempts
	Type	DisplayString
npAnswerTime	OID	3
	Description	Answer Time
	Type	DisplayString
npBridgeName	OID	4
	Description	Bridge Name
	Type	DisplayString
npCallAnswered	OID	5
	Description	Call Answered
	Type	DisplayString
npCallCapacityGroup	OID	6
	Description	Call Capacity Group
	Type	DisplayString
npCallId	OID	7
	Description	Call ID
	Type	DisplayString
npCallPersonality	OID	8
	Description	Call Personality
	Type	DisplayString
npCalledNumber	OID	9
	Description	Called Number
	Type	DisplayString
npCalledNumberContext	OID	10

Parameter Name	Attributes	Values
	Description	Called Number Context
	Type	DisplayString
npCaller	OID	11
	Description	Caller
	Type	DisplayString
npCallingNumber	OID	12
	Description	Calling Number
	Type	DisplayString
npCallingNumberContext	OID	13
	Description	Calling Number Context
	Type	DisplayString
npCallingPartyCategory	OID	14
	Description	Calling Party Category
	Type	DisplayString
npCallingPresentationIndicator	OID	15
	Description	Calling Presentation Indicator
	Type	DisplayString
npCallsLimit	OID	16
	Description	Calls Limit
	Type	DisplayString
npCallTreatment	OID	17
	Description	Call Treatment
	Type	DisplayString
npCallType	OID	18
	Description	Call Type
	Type	DisplayString
npClientAddress	OID	19
	Description	Client Address
	Type	DisplayString
npClusterName	OID	20
	Description	Cluster Name
	Type	DisplayString
npConfiguredAddress	OID	21
	Description	Configured Address
	Type	DisplayString

Parameter Name	Attributes	Values
npConfiguredPhysicalLocation	OID	22
	Description	Configured Physical Location
	Type	DisplayString
npCounterName	OID	23
	Description	Counter Name
	Type	DisplayString
npCountryCode	OID	24
	Description	Country Code
	Type	DisplayString
npCpuIdleTimePercentage	OID	25
	Description	CPU Idle Time Percentage
	Type	DisplayString
npCurrentThresholdValue	OID	26
	Description	Current Threshold Value
	Type	DisplayString
npDate	OID	27
	Description	Date
	Type	DisplayString
npDepartmentName	OID	28
	Description	Department Name
	Type	DisplayString
npDestinationUserId	OID	29
	Description	Destination User ID
	Type	DisplayString
npDeviceAddress	OID	30
	Description	Device Address
	Type	DisplayString
npDeviceLinePort	OID	31
	Description	Device Line Port
	Type	DisplayString
npDeviceList	OID	32
	Description	Device List
	Type	DisplayString
npDeviceName	OID	33
	Description	Device Name

Parameter Name	Attributes	Values
	Type	DisplayString
npDeviceType	OID	34
	Description	Device Type
	Type	DisplayString
npDialedNumber	OID	35
	Description	Dialed Number
	Type	DisplayString
npDirection	OID	36
	Description	Direction
	Type	DisplayString
npDomain	OID	37
	Description	Domain
	Type	DisplayString
npEndpointId	OID	38
	Description	Endpoint ID
	Type	DisplayString
npExceptionMessage	OID	39
	Description	Exception Message
	Type	DisplayString
npExpectedVersion	OID	40
	Description	Expected Version
	Type	DisplayString
npFailedAttempts	OID	41
	Description	Failed Attempts
	Type	DisplayString
npFailedLoginAttempts	OID	42
	Description	Failed Login Attempts
	Type	DisplayString
npFeatureName	OID	43
	Description	Feature Name
	Type	DisplayString
npFilename	OID	44
	Description	File Name
	Type	DisplayString
npFilenameAlt	OID	45

Parameter Name	Attributes	Values
	Description	Alternate File Name
	Type	DisplayString
npFirstName	OID	46
	Description	First Name
	Type	DisplayString
npGaugeName	OID	47
	Description	Gauge Name
	Type	DisplayString
npGroupId	OID	48
	Description	Group ID
	Type	DisplayString
npGroupName	OID	49
	Description	Group Name
	Type	DisplayString
npGroupNumber	OID	50
	Description	Group Number
	Type	DisplayString
npHost	OID	51
	Description	Host
	Type	DisplayString
npIndex	OID	52
	Description	Index
	Type	DisplayString
npInhibitedNeighbors	OID	53
	Description	Inhibited Neighbours
	Type	DisplayString
npInstanceName	OID	54
	Description	Instance Name
	Type	DisplayString
npLastIncomingCallTime	OID	55
	Description	Last Incoming Call Time
	Type	DisplayString
npLastName	OID	56
	Description	Last Name
	Type	DisplayString

Parameter Name	Attributes	Values
npLicenseAllocation	OID	57
	Description	License Allocation
	Type	DisplayString
npLicenseKey	OID	58
	Description	License Key
	Type	DisplayString
npLicenseLimit	OID	59
	Description	License Limit
	Type	DisplayString
npLocalInterface	OID	60
	Description	Local Interface
	Type	DisplayString
npLocalPort	OID	61
	Description	Local Port
	Type	DisplayString
npMailboxId	OID	62
	Description	Mailbox ID
	Type	DisplayString
npMaxFailedLoginAttempts	OID	63
	Description	Maximum Failed Login Attempts
	Type	DisplayString
npMessage	OID	64
	Description	Message
	Type	DisplayString
npMethod	OID	65
	Description	Method
	Type	DisplayString
npMissingHeader	OID	66
	Description	Missing Header
	Type	DisplayString
npNbDevicesProcessed	OID	67
	Description	Number of Devices Processed
	Type	DisplayString
npNbDevicesWithoutMACAddress	OID	68
	Description	Number of Devices Without MAC Address

Parameter Name	Attributes	Values
	Type	DisplayString
npNbInhibitedNeighbors	OID	69
	Description	Number of Inhibited Neighbors
	Type	DisplayString
npNbOfErrors	OID	70
	Description	Number of Errors
	Type	DisplayString
npNbOfSoapThreads	OID	71
	Description	Number of SOAP Threads
	Type	DisplayString
npNbTransactions	OID	72
	Description	Number of Transactions
	Type	DisplayString
npNetworkCallId	OID	73
	Description	Network Call ID
	Type	DisplayString
npNewAddress	OID	74
	Description	New Address
	Type	DisplayString
npNewAdministrativeState	OID	75
	Description	New Administrative State
	Type	DisplayString
npNewDomainName	OID	76
	Description	New Domain Name
	Type	DisplayString
npNewOperationalState	OID	77
	Description	New Operational State
	Type	DisplayString
npNewThresholdValue	OID	78
	Description	New Threshold Value
	Type	DisplayString
npNewZone	OID	79
	Description	New Zone
	Type	DisplayString
npNodeId	OID	80

Parameter Name	Attributes	Values
	Description	Node ID
	Type	DisplayString
npOldAdministrativeState	OID	81
	Description	Old Administrative State
	Type	DisplayString
npOldDomainName	OID	82
	Description	Old Domain Name
	Type	DisplayString
npOldOperationalState	OID	83
	Description	Old Operational State
	Type	DisplayString
npOldZone	OID	84
	Description	Old Zone
	Type	DisplayString
npOperation	OID	85
	Description	Operation
	Type	DisplayString
npOriginalAddress	OID	86
	Description	Original Address
	Type	DisplayString
npOriginalCalledNumber	OID	87
	Description	Original Called Number
	Type	DisplayString
npOriginalCalledNumberContext	OID	88
	Description	Original Called Number Context
	Type	DisplayString
npOriginalCalledNumberPresentationIndicator	OID	89
	Description	Original Called Number Presentation Indicator
	Type	DisplayString
npOriginalCalledReason	OID	90
	Description	Original Called Reason
	Type	DisplayString
npOriginator	OID	91
	Description	Originator
	Type	DisplayString

Parameter Name	Attributes	Values
npPeriod	OID	92
	Description	Period
	Type	DisplayString
npPolicyFeature	OID	93
	Description	Policy Feature
	Type	DisplayString
npProtocol	OID	94
	Description	Protocol
	Type	DisplayString
npReason	OID	95
	Description	Reason
	Type	DisplayString
npRadiusServerList	OID	96
	Description	Radius Server List
	Type	DisplayString
npReceivedPhysicalLocation	OID	97
	Description	Received Physical Location
	Type	DisplayString
npReceivedVersion	OID	98
	Description	Received Version
	Type	DisplayString
npRedirectingNumber	OID	99
	Description	Redirecting Number
	Type	DisplayString
npRedirectingNumberContext	OID	100
	Description	Redirecting Number Context
	Type	DisplayString
npRedirectingNumberPresentation Indicator	OID	101
	Description	Redirecting Number Presentation Indicator
	Type	DisplayString
npRedirectingReason	OID	102
	Description	Redirecting Reason
	Type	DisplayString
npRemoteAddress	OID	103
	Description	Remote Address

Parameter Name	Attributes	Values
	Type	DisplayString
npRemoteParty	OID	104
	Description	Remote Party
	Type	DisplayString
npRemotePort	OID	105
	Description	Remote Port
	Type	DisplayString
npReport	OID	106
	Description	Report
	Type	DisplayString
npRequest	OID	107
	Description	Request
	Type	DisplayString
npResolvedAddress	OID	108
	Description	Resolved Address
	Type	DisplayString
npRoute	OID	109
	Description	Route
	Type	DisplayString
npServerName	OID	110
	Description	Server Name
	Type	DisplayString
npServerType	OID	111
	Description	Server Type
	Type	DisplayString
npServiceProviderId	OID	112
	Description	Service Provider ID
	Type	DisplayString
npSessionId	OID	113
	Description	Session ID
	Type	DisplayString
npSessionKey	OID	114
	Description	Session Key
	Type	DisplayString
npSipErrorCode	OID	115

Parameter Name	Attributes	Values
	Description	SIP Error Code
	Type	DisplayString
npSipRequestMessage	OID	116
	Description	SIP Request Message
	Type	DisplayString
npSipResponseMessage	OID	117
	Description	SIP Response Message
	Type	DisplayString
npSizeLimit	OID	118
	Description	Size Limit
	Type	DisplayString
npSmdiNumber	OID	119
	Description	SMDI Number
	Type	DisplayString
npStackTrace	OID	120
	Description	Stack Trace
	Type	DisplayString
npStartTime	OID	121
	Description	Start Time
	Type	DisplayString
npSubscriberType	OID	122
	Description	Subscriber Type
	Type	DisplayString
npTaskName	OID	123
	Description	Task Name
	Type	DisplayString
npThreadName	OID	124
	Description	Thread Name
	Type	DisplayString
npThresholdName	OID	125
	Description	Threshold Name
	Type	DisplayString
npTimeElapsed	OID	126
	Description	Time Elapsed
	Type	DisplayString

Parameter Name	Attributes	Values
npTimeLength	OID	127
	Description	Time Length
	Type	DisplayString
npTimestamp	OID	128
	Description	Timestamp
	Type	DisplayString
npTraceType	OID	129
	Description	Trace Type
	Type	DisplayString
npTrunkGroupName	OID	130
	Description	Trunk Group Name
	Type	DisplayString
npUrl	OID	131
	Description	Uniform Resource Locator
	Type	DisplayString
npUserId	OID	132
	Description	User ID
	Type	DisplayString
npUserName	OID	133
	Description	User Name
	Type	DisplayString
npUserNumber	OID	134
	Description	User Number
	Type	DisplayString
npUserUid	OID	135
	Description	User UID
	Type	DisplayString
npThresholdDescription	OID	136
	Description	Threshold Description
	Type	DisplayString
npSubscriberId	OID	137
	Description	Subscriber ID
	Type	DisplayString
npCommand	OID	138
	Description	Command

Parameter Name	Attributes	Values
	Type	DisplayString
npPublicIdentity	OID	139
	Description	Public Identity
	Type	DisplayString
npDataReference	OID	140
	Description	Data Reference
	Type	DisplayString
npResultCode	OID	141
	Description	Result Code
	Type	DisplayString
npResultCodeType	OID	142
	Description	Result Code Type
	Type	DisplayString
npError	OID	143
	Description	Error
	Type	DisplayString
npLoginLevel	OID	144
	Description	Login Level
	Type	DisplayString
npMaximumNbItems	OID	145
	Description	Maximum Number of Items
	Type	DisplayString
npRequestUriUser	OID	146
	Description	Requested User URI
	Type	DisplayString
npWebAppContext	OID	147
	Description	Web Application context path
	Type	DisplayString
npTreatment	OID	148
	Description	Treatment received for call
	Type	DisplayString
npPrimaryAddress	OID	149
	Description	Primary Address
	Type	DisplayString
npSecondaryAddress	OID	150

Parameter Name	Attributes	Values
	Description	Secondary Address
	Type	DisplayString
npServiceProviderName	OID	151
	Description	Service Provider Name
	Type	DisplayString
npConfigVersion	OID	152
	Description	Configuration revision number
	Type	DisplayString
npApplicationName	OID	153
	Description	Name of the application.
	Type	DisplayString
npOldEffectiveState	OID	154
	Description	Old Effective State
	Type	DisplayString
npNewEffectiveState	OID	155
	Description	New Administrative State
	Type	DisplayString
npApplicationMemory	OID	156
	Description	The quantity of memory allocated for the application.
	Type	DisplayString
npSystemMemory	OID	157
	Description	The total amount of memory in the system that is available to allocate for applications.
	Type	DisplayString
npSourceCodec	OID	158
	Description	Name of original codec.
	Type	DisplayString
npDestinationCodec	OID	159
	Description	Name of destination codec.
	Type	DisplayString
npMaximumAttempt	OID	160
	Description	Maximum number of attempt.
	Type	DisplayString
npMacAddress	OID	161
	Description	Mac Address

Parameter Name	Attributes	Values
	Type	DisplayString
npMaxNumberOfSessions	OID	162
	Description	Maximum number of sessions
	Type	DisplayString
npSACGroupId	OID	163
	Description	The Id of the SAC group
	Type	DisplayString
npFileURL	OID	164
	Description	The file URL
	Type	DisplayString
npObjectId	OID	165
	Description	Object Identifier
	Type	DisplayString
npMSCAddr	OID	166
	Description	network MSC Address
	Type	DisplayString
npRoutePointName	OID	167
	Description	The name of the route point
	Type	DisplayString
npProfileDescription	OID	168
	Description	The profile description
	Type	DisplayString
npTransactionLimitPeriod	OID	169
	Description	The transaction limit period in secs
	Type	DisplayString
npGlobalTransactionLimit	OID	170
	Description	The configured global transaction limit
	Type	DisplayString
npNetAddress	OID	171
	Description	The IP/FQDN Address
	Type	DisplayString
npReportName	OID	172
	Description	The name of the scheduled report. This parameter is encoded using the application/x-www-form-urlencoded MIME format.
	Type	DisplayString

Parameter Name	Attributes	Values
npDateTime	OID	173
	Description	The date and time
	Type	DisplayString
npTimeoutValue	OID	174
	Description	The timeout value
	Type	DisplayString
npMediaServerAddress	OID	175
	Description	The address of the Media Server.
	Type	DisplayString
npUserDN	OID	176
	Description	The DN of the paging group.
	Type	DisplayString
npApplicationServerSetName	OID	177
	Description	The Application Server set name
	Type	DisplayString
npApplicationServerSetContent	OID	178
	Description	A comma-separated list of Hosting NE names that are part of the set.
	Type	DisplayString
npIdentity	OID	179
	Description	The main PUI for the profile.
	Type	DisplayString
npAlternate	OID	180
	Description	The alternate PUI which failed to be linked.
	Type	DisplayString
npDatabaseName	OID	181
	Description	The database name.
	Type	DisplayString
npSite	OID	182
	Description	The database site.
	Type	DisplayString
npEnterpriseId	OID	183
	Description	The enterprise Id.
	Type	DisplayString
npAddress	OID	184

Parameter Name	Attributes	Values
	Description	The IP address.
	Type	DisplayString
npResourceRecordType	OID	185
	Description	Resource record type (NAPTR, SRV, A, PTR) in the query.
	Type	DisplayString
npIMRNNumber	OID	186
	Description	IMRN number
	Type	DisplayString
npSIPCallID	OID	187
	Description	SIP Call ID
	Type	DisplayString
npFrom	OID	188
	Description	Caller
	Type	DisplayString
npDatabaseObjectType	OID	189
	Description	Database Object type.
	Type	DisplayString
npWebAppName	OID	190
	Description	Web Application Name
	Type	DisplayString
npBroadCloudRequest	OID	191
	Description	The provisioning action requested to BroadCloud. Can be POST, PUT or DELETE
	Type	DisplayString
npBroadCloudUid	OID	192
	Description	The BroadCloud unique subscriber id.
	Type	DisplayString
npBroadCloudService	OID	193
	Description	The BroadCloud service for which the request was made.
	Type	DisplayString
npBroadCloudFailureReason	OID	194
	Description	The reason for the failure.
	Type	DisplayString
npSCCASPSIDNNumber	OID	195
	Description	SCC AS PSI DN number.

Parameter Name	Attributes	Values
	Type	DisplayString
npDBSchemaName	OID	196
	Description	The name of the database schema instance.
	Type	DisplayString
npHttpWorkersBusy	OID	197
	Description	The ratio of busy workers.
	Type	DisplayString
npExecutorType	OID	198
	Description	The executor type (ajp, httpnio, cti, ocic, ocip).
	Type	DisplayString
npExecutorQueueUsage	OID	199
	Description	The ratio of executor queue usage.
	Type	DisplayString
npExecutorQueueLatency	OID	200
	Description	The ratio of executor queue latency.
	Type	DisplayString
npExecutorDurationUnit	OID	201
	Description	The measurement unit.
	Type	DisplayString
npExecutorThreadPoolProcessingTime	OID	202
	Description	The executor thread pool processing time.
	Type	DisplayString
npExecutorThreadPoolProcessing DurationUnit	OID	203
	Description	The executor thread pool processing time unit.
	Type	DisplayString
npExecutorThreadPoolBusy	OID	204
	Description	The executor thread pool busy ratio.
	Type	DisplayString
npProcessMemoryUsage	OID	205
	Description	The process memory usage.
	Type	DisplayString
npReceivedRequestsDuringLastPeriod	OID	206
	Description	The number of requests received during the last overload protection period.
	Type	DisplayString

Parameter Name	Attributes	Values
npProtectionPeriod	OID	207
	Description	The duration of the overload protection period.
	Type	DisplayString
npPeriodUnit	OID	208
	Description	The unit used for the overload protection period. Its default value is seconds.
	Type	DisplayString
npWebAppUser	OID	209
	Description	The user of the web app
	Type	DisplayString
npNEMaintenancePartitionId	OID	210
	Description	The subscriber's NE maintenance partition
	Type	DisplayString
sccpObjId	OID	211
	Description	The sccp object id
	Type	Integer32
sccpState	OID	212
	Description	The sccp state
	Type	Integer32
sccpAffectedSsn	OID	213
	Description	The sccp affected sub system number
	Type	Integer32
sccpAffectedSsnSp	OID	214
	Description	The sp of affected sub system number
	Type	Integer32
sccpAffectedSsnSsn	OID	215
	Description	The affected sub system number
	Type	Integer32
sccpConnectionId	OID	216
	Description	The sccp connection id
	Type	Integer32
sccpResetReason	OID	217
	Description	The sccp reset reason
	Type	DisplayString
sccpOriginator	OID	218

Parameter Name	Attributes	Values
	Description	The sccp originator
	Type	DisplayString
sccpModuleId	OID	219
	Description	The sccp module id
	Type	Integer32
sccpSubModuleId	OID	220
	Description	The sccp sub-module id
	Type	Integer32
sccpMtpSap	OID	221
	Description	The sap id
	Type	Integer32
sccpErrorCode	OID	222
	Description	The sccp error code
	Type	Integer32
sccpBitMask	OID	223
	Description	The sccp bit mask
	Type	Integer32
sccpDroppedApiId	OID	224
	Description	The sccp dropped api id
	Type	Integer32
sccpErrorLevel	OID	225
	Description	The sccp error level
	Type	Integer32
sccpErrorFlag	OID	226
	Description	The sccp error flag
	Type	Integer32
sccpPointCode	OID	227
	Description	The point code
	Type	Integer32
m3uaAsId	OID	228
	Description	The m3ua AS id
	Type	Integer32
m3uaLocalSpId	OID	229
	Description	The m3ua local SP id
	Type	Integer32

Parameter Name	Attributes	Values
m3uaRemSpId	OID	230
	Description	The m3ua remote SP id
	Type	Integer32
m3uaState	OID	231
	Description	The m3ua state
	Type	DisplayString
m3uaNwSpId	OID	232
	Description	The m3ua n/w SP id
	Type	Integer32
m3uaAspId	OID	233
	Description	The m3ua ASP id
	Type	Integer32
m3uaOptIndParams	OID	234
	Description	The m3ua optional indication paramters
	Type	Integer32
m3uaOptIndParamsBitmap	OID	235
	Description	The m3ua optional indication paramter's bitmap
	Type	Integer32
m3uaOptIndParamsDownCause	OID	236
	Description	The m3ua optional indication paramter's down cause
	Type	Integer32
m3uaSgId	OID	237
	Description	The m3ua SG id
	Type	Integer32
m3uaAssocId	OID	238
	Description	The association id
	Type	Integer32
m3uaNumInStreams	OID	239
	Description	The number of input streams
	Type	Integer32
m3uaNumOutStreams	OID	240
	Description	The number of output streams
	Type	Integer32
m3uaErrSrc	OID	241
	Description	The m3ua error source

Parameter Name	Attributes	Values
	Type	Integer32
m3uaEcode	OID	242
	Description	The m3ua error code
	Type	Integer32
m3uaInfoLength	OID	243
	Description	The m3ua information length
	Type	Integer32
m3uaPInfoStr	OID	244
	Description	The m3ua information string
	Type	OCTET STRING
m3uaRegStatus	OID	245
	Description	The m3ua registration status
	Type	Integer32
m3uaDeregStatus	OID	246
	Description	The m3ua de-registration status
	Type	Integer32
m3uaNewAs	OID	247
	Description	The m3ua new AS
	Type	Integer32
m3uaDelAs	OID	248
	Description	The m3ua deleted AS
	Type	Integer32
ss7pInstanceId	OID	249
	Description	The ss7p instance id
	Type	Integer32
ss7pStackType	OID	250
	Description	The ss7p stack type
	Type	Integer32
ss7pEcode	OID	251
	Description	The ss7p error code
	Type	Integer32
ss7pEntityStatus	OID	252
	Description	The ss7p entity status
	Type	DisplayString
ss7pFailureEcode	OID	253

Parameter Name	Attributes	Values
	Description	The ss7p failure error code
	Type	Integer32
ss7pTierId	OID	254
	Description	The ss7p tier id
	Type	Integer32
ss7pPc	OID	255
	Description	The ss7p point code
	Type	Integer32
ss7pPcType	OID	256
	Description	The ss7p point code type
	Type	Integer32
ss7pSpId	OID	257
	Description	The ss7p SP id
	Type	Integer32
ss7pNi	OID	258
	Description	The ss7p network indicator
	Type	Integer32
ss7pVariant	OID	259
	Description	The ss7p variant
	Type	DisplayString
ss7pSapId	OID	260
	Description	The ss7p sap id
	Type	Integer32
ss7pSsn	OID	261
	Description	The ss7p sub-system number
	Type	Integer32
ss7pSsId	OID	262
	Description	The ss7p sub-system id
	Type	Integer32
ss7pNumBitsInstanceId	OID	263
	Description	The ss7p T2 bits intance id
	Type	Integer32
ss7pFlag	OID	264
	Description	The ss7p flag
	Type	DisplayString

Parameter Name	Attributes	Values
ss7pEmStatus	OID	265
	Description	The ss7p EM status
	Type	DisplayString
ss7pEmInfoAddr	OID	266
	Description	The Em IP address
	Type	OCTET STRING (SIZE(30))
ss7pEmInfoServerPort	OID	267
	Description	The Em server port
	Type	Integer32
ss7pEmInfoMinClientPort	OID	268
	Description	The Em minimum client port
	Type	Integer32
ss7pEmInfoMaxClientPort	OID	269
	Description	The Em maximum client port
	Type	Integer32
ss7pInstanceType	OID	270
	Description	The ss7p instance type
	Type	DisplayString
ss7pIp	OID	271
	Description	The ss7p IP address
	Type	OCTET STRING (SIZE(20))
ss7pPort	OID	272
	Description	The Ss7p port
	Type	Integer32
ss7pIpStr	OID	273
	Description	The ss7p IP address in string
	Type	OCTET STRING (SIZE(20))
mapInstId	OID	274
	Description	The map instance id
	Type	Integer32
mapTierLevel	OID	275
	Description	The map platform tier level
	Type	Integer32
mapErrorCode	OID	276
	Description	The map error code

Parameter Name	Attributes	Values
	Type	Integer32
mapInfoLen	OID	277
	Description	The map information length
	Type	Integer32
mapInfoStr	OID	278
	Description	The Em information string
	Type	OCTET STRING
mapStatus	OID	279
	Description	The map status
	Type	DisplayString
mapInstanceType	OID	280
	Description	The map instance type
	Type	DisplayString
mapVariant	OID	281
	Description	The map platform variant
	Type	Integer32
mapIp	OID	282
	Description	The map ip address
	Type	OCTET STRING (SIZE(30))
mapPort	OID	283
	Description	The map port
	Type	Integer32
mapEmStatus	OID	284
	Description	The map EM status
	Type	DisplayString
mapEmInfoAddr	OID	285
	Description	The map EM's IP address
	Type	OCTET STRING (SIZE(30))
mapEmInfoServerPort	OID	286
	Description	The map EM's server port
	Type	Integer32
mapEmInfoMinClientPort	OID	287
	Description	The map EM's minimum client port
	Type	Integer32
mapEmInfoMaxClientPort	OID	288

Parameter Name	Attributes	Values
	Description	The map EM's maximum client port
	Type	Integer32
npSecureTlktToolName	OID	289
	Description	The name of the Secure Toolkit.
	Type	DisplayString
npSecureTlktToolResult	OID	290
	Description	The result of the Secure Toolkit.
	Type	DisplayString
npIMRN	OID	291
	Description	The IP Multimedia Routing Number.
	Type	DisplayString
npDeviceLinePortOrPublicIdentity	OID	292
	Description	The Device Line/Port or Public Identity.
	Type	DisplayString
npLockoutCounter	OID	293
	Description	The lockout count since last reset.
	Type	DisplayString
npLockoutPeriod	OID	294
	Description	The number of minutes or permanent.
	Type	DisplayString
npDeviceProfileName	OID	295
	Description	The Device Profile Name.
	Type	DisplayString
npDeviceFileRequestMessage	OID	296
	Description	The Device File Request Message.
	Type	DisplayString
npWebAppContextPath	OID	297
	Description	The Web Application context path.
	Type	DisplayString
npSS7SubsystemNumber	OID	298
	Description	The SS7 Subsystem number.
	Type	DisplayString
npAuthenticationServer	OID	299
	Description	The authentication server.
	Type	DisplayString

Parameter Name	Attributes	Values
npLdapVersion	OID	300
	Description	The configured LDAP version.
	Type	DisplayString
npSchemaInstanceName	OID	301
	Description	The schema instance name.
	Type	DisplayString
npSchemaInstanceState	OID	302
	Description	The schema instance state.
	Type	DisplayString
npMessageCount	OID	303
	Description	The number of Messages.
	Type	DisplayString
npProfileServer	OID	304
	Description	The ProfileServer.
	Type	DisplayString
npPercentEventQueueFiles	OID	305
	Description	The percentage of event queue files in use.
	Type	DisplayString
npMaxNumEventQueueFiles	OID	306
	Description	The Maximum number of event queue files allowed.
	Type	DisplayString
npOldestEventAge	OID	307
	Description	The age of oldest event not saved on the Database Server.
	Type	DisplayString
npMaxEventAge	OID	308
	Description	The maximum age of an event that can be saved on the Database Server.
	Type	DisplayString
npLogFile	OID	309
	Description	The log filename.
	Type	DisplayString
npIS41Operation	OID	310
	Description	The IS41 operation.
	Type	DisplayString
npMissingComponent	OID	311

Parameter Name	Attributes	Values
	Description	The missing component.
	Type	DisplayString
npState	OID	312
	Description	The state id the component.
	Type	DisplayString
npExistingComponent	OID	313
	Description	The existing component.
	Type	DisplayString
npBridgeParticipantId	OID	314
	Description	The bridge participant id.
	Type	DisplayString
npRoomId	OID	315
	Description	The room id.
	Type	DisplayString
npErrorCode	OID	316
	Description	The error code.
	Type	DisplayString
npErrorMessage	OID	317
	Description	The error message.
	Type	DisplayString
npPort	OID	318
	Description	The Port.
	Type	DisplayString
npName	OID	319
	Description	The name of the Hypertext Transfer Protocol (HTTP) server or the Internet Protocol (IP) address for other protocols.
	Type	DisplayString
npRepositoryUri	OID	320
	Description	The URI of the repository.
	Type	DisplayString
npRemoteAddresses	OID	321
	Description	The remote addresses.
	Type	DisplayString
npConnectionType	OID	322
	Description	The connection type.

Parameter Name	Attributes	Values
	Type	DisplayString
npFileCapacityInBytes	OID	323
	Description	The capacity of a file in bytes.
	Type	DisplayString
npFileSystemPathList	OID	324
	Description	The list of paths.
	Type	DisplayString
npDiskUsageInBytes	OID	325
	Description	The amount of disk space currently in use.
	Type	DisplayString
npValidLicenseId	OID	326
	Description	The valid license Id.
	Type	DisplayString
npNFMName	OID	327
	Description	The Network Function Manager name.
	Type	DisplayString
npNodeName	OID	328
	Description	The node name.
	Type	DisplayString
npLicenseIdInstance	OID	329
	Description	The details of the licenseId instance.
	Type	DisplayString
npNFMFqdn	OID	330
	Description	The Fully Qualified Domain Name (FQDN) of the Network Function Manager.
	Type	DisplayString
npBroadWorksRelease	OID	331
	Description	The BroadWorks release.
	Type	DisplayString
npGraceAction	OID	332
	Description	The action taken on grace period expiration.
	Type	DisplayString
npHours	OID	333
	Description	The number of hours remaining before taking action.
	Type	DisplayString

Parameter Name	Attributes	Values
npEnterpriseTrunkName	OID	334
	Description	The name of the enterprise trunk.
	Type	DisplayString
npInvalidLicenseId	OID	335
	Description	The invalid license Id.
	Type	DisplayString
npCallingParty	OID	336
	Description	The calling party.
	Type	DisplayString
npLicenseId	OID	337
	Description	The licenseId.
	Type	DisplayString
npContainerName	OID	338
	Description	The name of the container.
	Type	DisplayString
npDatabaseNode	OID	339
	Description	The hostname and port of the database node.
	Type	DisplayString
npDatabaseNodes	OID	340
	Description	A space separated list of all the hostname and port of the database nodes.
	Type	DisplayString
npQueueName	OID	341
	Description	The name of the queue.
	Type	DisplayString
npExtremeOverloadReason	OID	342
	Description	The reason for the extreme overload, either expiration or count.
	Type	DisplayString
npApplicationId	OID	343
	Description	The application ID.
	Type	DisplayString
npChannelId	OID	344
	Description	The Xsi channel Id.
	Type	DisplayString
npChannelSetId	OID	345

Parameter Name	Attributes	Values
	Description	The Xsi channel set id.
	Type	DisplayString
npChannelOwner	OID	346
	Description	The Xsi channel owner.
	Type	DisplayString
npRequestName	OID	347
	Description	The request name
	Type	DisplayString
npPatchTitle	OID	348
	Description	The patch title.
	Type	DisplayString
npListOfNodes	OID	349
	Description	The list of nodes.
	Type	DisplayString
npSWManagerVersion	OID	350
	Description	The Software Manager version.
	Type	DisplayString
npCallerAssertedIdentity	OID	351
	Description	The calling asserted identity, including the asserted name and number.
	Type	DisplayString
npCallingAssertedNumber	OID	352
	Description	The calling asserted number.
	Type	DisplayString
npCallingAssertedNumberContext	OID	353
	Description	The calling asserted number context.
	Type	DisplayString
npCurrentCounterValue	OID	354
	Description	The current value of the counter.
	Type	DisplayString
npClearThresholdValue	OID	355
	Description	The value to reach by the gauge to clear the alarm.
	Type	DisplayString
npCouchbaseNodes	OID	356
	Description	The List of Couchbase nodes.

Parameter Name	Attributes	Values
	Type	DisplayString
npTableName	OID	357
	Description	The name of the table that was modified.
	Type	DisplayString
npErrorText	OID	358
	Description	The error text.
	Type	DisplayString
npConnectionCount	OID	359
	Description	The number of connections.
	Type	Integer32
npDefaultProfilePUI	OID	360
	Description	The default user pui.
	Type	DisplayString
npDataCenter	OID	361
	Description	The name of the data center.
	Type	DisplayString
npResellerId	OID	362
	Description	The reseller id.
	Type	DisplayString
npTcapObjId	OID	363
	Description	The tcap object ID.
	Type	DisplayString
npTcapModuleId	OID	364
	Description	The tcap module ID.
	Type	DisplayString
npSs7pSapId	OID	365
	Description	The sap ID.
	Type	DisplayString
npTcapErrorCode	OID	366
	Description	The tcap error code.
	Type	DisplayString
npTcapErrorStr	OID	367
	Description	The tcap error string.
	Type	DisplayString
npTcapBitMask	OID	368

Parameter Name	Attributes	Values
	Description	The tcap bit mask.
	Type	DisplayString
npTcapUserId	OID	369
	Description	The tcap user ID.
	Type	DisplayString
npDialogId	OID	370
	Description	The dialog ID.
	Type	DisplayString
npDialogState	OID	371
	Description	The dialog state.
	Type	DisplayString
npTcapTransId	OID	372
	Description	The transaction ID.
	Type	DisplayString
npTcapTransState	OID	373
	Description	The transaction state.
	Type	DisplayString
npInvokeId	OID	374
	Description	The invoke ID.
	Type	DisplayString
npInvokeState	OID	375
	Description	The invoke state.
	Type	DisplayString
npResellerName	OID	376
	Description	The reseller name.
	Type	DisplayString
npPercent	OID	377
	Description	The percent.
	Type	DisplayString
npSourceOrFrom	OID	378
	Description	The IP address and port of the source or SIP URI of the caller.
	Type	DisplayString
npInterface	OID	379
	Description	The interface name.
	Type	DisplayString

Parameter Name	Attributes	Values
npThreshold	OID	380
	Description	The threshold value.
	Type	DisplayString
npTransport	OID	381
	Description	The transport used to send SIP OPTIONS.
	Type	DisplayString
npQueryDuration	OID	382
	Description	The query duration time.
	Type	DisplayString
npConfiguredMax	OID	383
	Description	The threshold time configured.
	Type	DisplayString
npDiscrepancyRatio	OID	384
	Description	The discrepancy ratio between the average execution time of a given command for the current run and the Life-Time average for this same command.
	Type	DisplayString
npCurrentAverage	OID	385
	Description	The current command average query time for this run.
	Type	DisplayString
npLifeTimeAverage	OID	386
	Description	The current command average query time over the life time of CallP Timing Verifications.
	Type	DisplayString
npBytes	OID	387
	Description	The number of bytes.
	Type	DisplayString
npLimitType	OID	388
	Description	The limit type that can be total, incoming or outgoing .
	Type	DisplayString
npConnectionPoolName	OID	389
	Description	The connection pool name.
	Type	DisplayString
npRemoteHostPort	OID	390
	Description	The remote address normalized.
	Type	DisplayString

Parameter Name	Attributes	Values
npSipEventMessage	OID	391
	Description	The SIP event remote address normalized.
	Type	DisplayString
npUserFullJid	OID	392
	Description	The user full JID.
	Type	DisplayString
npMucQueueRecords	OID	393
	Description	The number of records in the MUC queue table for the user resource in the last 1 minute.
	Type	DisplayString
npMucQueueTable	OID	394
	Description	The name of the MUC queue table.
	Type	DisplayString
npNbFiles	OID	395
	Description	Number of Files
	Type	DisplayString
npPartitionUsed	OID	396
	Description	The percentage of partition used.
	Type	DisplayString
npPartitionUsedLimit	OID	397
	Description	The percentage limit of partition used.
	Type	DisplayString
npHttpUrl	OID	398
	Description	The configured URL for the server.
	Type	DisplayString
npBcctConnection	OID	399
	Description	The BCCT connectiion.
	Type	DisplayString
npBcctProtocol	OID	400
	Description	The BCCT protocol.
	Type	DisplayString
npDocumentID	OID	401
	Description	The BCCT protocol.
	Type	DisplayString
npAdmin	OID	402

Parameter Name	Attributes	Values
	Description	The BCCT protocol.
	Type	DisplayString

Appendix B: bwSystemHealthReport Alarm Problem Text

The following table describes the problem text contained in the bwSystemHealthReport.

Problem text	Severity	Recommended action
The following FileSystems have exceeded the size limit: [STOPBW(<STOPBW_THRESHOLD>%) :: <PARTITION>] [CRITICAL(<CRITICAL_THRESHOLD>%) :: <PARTITION>] [HIGH(<HIGH_THRESHOLD>%) :: <PARTITION>] [WARNING(<WARNING_THRESHOLD>%) :: <PARTITION>]	Critical Critical Major Warning	Try to free up some space on FileSystems that have exceeded a limit. Consider deleting old logs, old database backups and/or old software versions in directories /var/broadworks/logs, /usr/local/broadworks and /bw/install. BroadSoft doesn't recommend keeping more that three software versions installed on a given server.
The following sub agents are not started: [MIBIISA sub agent] [ESD sub agent]	Minor	To start the SNMP sub agent(s): [As root user, do: /etc/init.d/init.subagentctl start] [As root user, do: /etc/init.d/init.es_agent start]
BroadWorks <server_type> processes in trouble:		
[Invalid date in BroadWorks License file.]	Minor	[Invalid date in BroadWorks License file, please contact BroadSoft Support.]
[BroadWorks License expired. License expire date:<expired_date>]	Minor	[BroadWorks License expired, please contact BroadSoft Support.]
[BroadWorks License expired. License expire date:<expired_date>]	Minor	[BroadWorks License is expiring, please contact BroadSoft Support.]
[SNMP Agent not running]	Critical	[Broadworks needs to be restarted]
[Configuration agent not running]	Critical	[The Configuration Agent needs to be restarted (configdctl start)]
[The Software Manager is not running]	Critical	[The Software Manager needs to be restarted (startswman.pl)]
[<CONTAINER_NAME> not running]	Critical	[The <FAULTY_APPLICATION> application needs to be restarted]
[<CONTAINER_NAME> process monitor not running]	Critical	[The <FAULTY_APPLICATION> application needs to be restarted]
[Current DSN permanent size (<PERM_SIZE>M) exceeds the maximum of 128M for a system with or with less than 1G in physical memory]	Major	[Contact BroadSoft Support to get the DSN resizing procedure]
[Current DSN permanent size (<PERM_SIZE>M) exceeds <MINIMUM_RATIO>\% of the memory available in the system <MEM_SIZE>M]	Major	[Contact BroadSoft Support to get the DSN resizing procedure]
[Open Client Server Monitoring not running]	Critical	[The Web Server needs to be restarted]
[Open Client Server not running]	Critical	[The Web Server needs to be restarted]
[APACHE Monitoring not running]	Critical	[The Web Server needs to be restarted]
[APACHE not running]	Critical	[The Web Server needs to be restarted]
[Flash policy server process monitor not running]	Critical	[The Web Server needs to be restarted]
[Flash policy server not running]	Critical	[The Web Server needs to be restarted]
[<PROCESS_NAME> process monitor not running]	Critical	[The <SERVER_TYPE> needs to be restarted]

Problem text	Severity	Recommended action
[<PROCESS_NAME> not running]	Critical	[The <SERVER_TYPE> needs to be restarted]
[License Server process monitor not running]	Critical	[The Virtualized License Server needs to be restarted]
[License Server not running]	Critical	[The Virtualized License Server needs to be restarted]
[DbManagement not running]	Critical	[The Database Server needs to be restarted. Please restart BroadWorks server using restartbw.]
[SSHD not running]	Critical	[Restart the sshd process (/etc/init.d/sshd start)]
[TIMESTEND not running]	Critical	[The TimesTen daemon (TIMESTEND) needs to be restarted. Please refer to the BroadWorks Maintenance Guide for detailed procedures on how to restart the process(es) currently not running on this server, or contact your BroadWorks support team.]
[*** Internal error in healthmon script *** <INTERNAL_ERROR_OUTPUT>]	Major	[Contact BroadSoft support.]
[Could not properly monitor TimesTen permanent and temporary memory area usage. This error is not fatal and can be caused by an impossibility to obtain a connection to the TimesTen engine.]	Minor	Try running “<command>” and see if you get any results. If this problem persists, please contact BroadSoft support.
[TimesTen permanent memory area is at <PERM_MEM_PERCENT> of total permanent size. (Currently in use size is at <PERM_IN_USE>. Allocated size is <ALLOCATED_SIZE>, high water mark is <HIGH_WATER_MARK> and in use size is <PERM_IN_USE>]	Critical, Major or Minor	[Increase your datastore permanent size area (using the resizeDSN tool]
[TimesTen temporary memory area is at <TEMP_MEM_PERCENT> of total temporary size. (Currently in use size is at <TEMP_IN_USE>. Allocated size is <ALLOCATED_SIZE>, high water mark is <HIGH_WATER_MARK> and in use size is <TEMP_IN_USE>]	Critical, Major or Minor	[Increase your datastore temporary size area (using the resizeDSN tool)]
[TimesTen data store permanent size is different (<PERM_ALLOCATED> compared to <CURRENT>) on peers in the cluster.]	Critical	[Check the data store permanent size and adjust it so that all peers have the same permanent size (using the resizeDSN tool).]
[TimesTen data store temporary size is different (<PERM_ALLOCATED> compared to <CURRENT>) on peers in the cluster.]	Critical	[Check the data store temporary size and adjust it so that all peers have the same temporary size (using the resizeDSN tool).]
[SLAPD not running]	Critical	[Restart the slapd process (/etc/init.d/ldapctl start)]
[An error occured with the LDAP server replication.]	Critical	[Restart the LDAP server replication by importing the database on the secondary from the primary.]
[Cannot connect to the LDAP master server to retrieve replication status.]	Critical	[Configure LDAP master and slave server with same replication port.]
[Cannot connect to the LDAP slave server to retrieve replication status.]	Critical	[Configure LDAP master and slave server with same replication port.]
[MYSQLD is not running]	Critical	[The MySQL daemon (MYSQLD) needs to be restarted. Please refer to the BroadWorks Maintenance Guide for detailed procedures on how to restart the process(es) currently not running on this server, or contact BroadSoft support team.]

Problem text	Severity	Recommended action
[Database integrity failed]	Critical	[The MySQL database needs to be repaired: <OUTPUT_MSG>. Please restart BroadWorks server using restartbw command to repair the database. If the problem persist, contact BroadSoft support team.]
[DSN not initialized properly.]	Critical	[The server must be re-installed. If the problem persist, contact BroadSoft support team.]
[Application schema not properly installed.]	Critical	[The server must be re-installed. If the problem persist, contact BroadSoft support team.]
[Oracle DBS Utilities Error Detected]	Critical	[The server must be re-installed. If the problem persist, contact BroadSoft support team.]
[Oracle Grid not running.]	Critical	[Oracle Grid Infrastructure (High Availability framework) needs to be restarted]
[Fragmentation detected on <ENTITY>.]	Warning	[Contact BroadSoft Support]
[Low preallocation level detected on <ENTITY>]	Warning	[Contact BroadSoft Support]
[<NUM_OF_ERROR> Oracle redo log checkpointing error(s) detected.]	Major	[Contact BroadSoft Support]
[Oracle Observer not running]	Major	[Oracle Observer needs to run on a separate server (PS) and must be configured to monitor this DBS.]
[Oracle Database failover detected]	Major	[Restore the original primary site and perform a manual switch-over using the DBS observer CLI]
[Oracle redundancy error detected, failure on the primary site will result in data loss.]	Major	[Make sure redo apply is enabled by running 'dbsctl redo apply=on' on the standby site. If the error persists, contact BroadSoft Support.]
[Oracle Database secondary host <HOST_NAME> is not ready.]	Warning	[Verify <HOST> reacheability or reinstall a new standby and reconfigure redundancy.]
[Could not found an active primary database instance.]	Major	[Log back as bwadmin on the primary DBS to complete redundancy configuration.]
[Could not get reliable peer information.]	Major	[Please restart BroadWorks server using restartbw.]
[Oracle Database not running.]	Critical	[Oracle Database must be restarted.]
[Internal: problem with healthmon script (validate_peers_state method)]	Critical	[Contact BroadSoft Support.]
[Error in transmitting commands to a remote peer. Reported error is: <ERROR>]	Critical	[Make sure ssh and replication are correctly configured. (If a server has been unreachable for a long time, its database may be out-of-synch. It can be re-synchronized with importdb.pl. Please refer to the BroadWorks Maintenance Guide.]
[Replication: a remote server is in MAINTENANCE state. Replication test bypassed.]	Warning	[Validate that the peer server is in the right state.]
[Replication: a remote server <PEER> is not responding or not in RUNNING state. Replication test bypassed.]	Major	[Validate that the peer server <PEER> is reachable.]
[File replication is not running.]	Critical	[Perform a file replication restart (repctl restart)]
[Cannot connect to the MySQL database to retrieve replication status.]	Critical	[Contact BroadSoft Support.]
[An error occured with the database replication.]	Critical	[Restart the database replication by importing the database on the secondary from the primary.]

Problem text	Severity	Recommended action
[The following peers' clocks have a delay of +/- <DIFFERENCE> seconds with the local (<LOCAL_HOSTNAME>) clock: <PEER_LIST>]	Minor	[Make sure that the clocks are synchronized. If using NTP, ensure that all peers are using the same server. If using NTP with the same server, augment the frequency at which the time is synchronized with the server for each peer.]
[Not all members of the cluster use the same SWManager version.]	Minor	[Make sure that all of this server's peers are running the same SWManager version.]
[All members of this cluster are not at the same patch level.]	Major	[The output of the checkPeer.pl script returned the following output: <OUTPUT>. All servers in a cluster must be at the same patch level.]
[Hostname <HOSTNAME> cannot be found in redundancy peers (peerctl ls)]	Major	[Change the server hostname or change the redundancy peer hostname (peerctl)]
[Database is locked: no provisioning can occur on the server]	Major	[Unlock the server using peerctl]
[Server is NOT unlocked]	Major	[Unlock the server via the CLI or SNMP.]
[Failure in reading server administrative state from the Configuration Agent]	Major	[Make sure the Configuration Agent is started (configdctl status)]
[Unknown server state received from server: <STATE>]	Major	[Make sure the SNMP Agent is started (snmpdctl status)]
[The directory for offline CDR file queueing (/var/broadworks/billing/rf/) takes more than 5% of the available space on the partition where it is mounted. File queuing will be disabled.]	Minor	[File Queuing could not be automatically disabled. Manually disable it at the CLI: AS_CLI/Interface/Accounting/BroadWorksCDRInterface/Diameter/Offline> set enableFileQueuing false. Manually re-enable file queuing when the disk full condition is cleared. Verify that the file queuing retention time is appropriate for the call rate and the disk space. Verify that the listed offline charging servers are up and running. Verify that there is network connection between the Application Server and the offline charging servers. Verify that the Diameter interface is properly configured on the Application Server.]
[The partition on which the directory for offline CDR file queueing (/var/broadworks/billing/rf/) is hosted is <PARTITION_USAGE>% full.]	Minor	[File Queuing could not be automatically disabled. Manually disable it at the CLI: AS_CLI/Interface/Accounting/BroadWorksCDRInterface/Diameter/Offline> set enableFileQueuing false. Manually re-enable file queuing when the disk full condition is cleared. Verify that the file queuing retention time is appropriate for the call rate and the disk space. Verify that the listed offline charging servers are up and running. Verify that there is network connection between the Application Server and the offline charging servers. Verify that the Diameter interface is properly configured on the Application Server.]
[Replication is not running for DSN <DSN>. Databases may be out-of-synch.]	Critical	[Replication must be started (repctl start). If databases are out-of-synch they must be re-synchronized first (with the importdb.pl tool). Please refer to the BroadWorks Maintenance Guide for detailed procedures.]
[Internal: problem with healthmon script (monitor_redundancy method)]	Critical	[Contact BroadSoft Support.]
[Insufficient space to perform backup]	Major	[Try to free up some space by deleting old logs, old database backups and/or old software versions.]

Problem text	Severity	Recommended action
[Dangling processes detected: <PROCESS_HEADER> <DANGLING_PROCESSES>]	Informational	[Over time dangling processes may cause performance impact on your BroadWorks system. Those processes were identified and killed automatically.]
[The swap configured on the system is very insufficient.]	Critical (50% of required swap detected) or Major (65% of required swap detected)	[You should add more swap space to the system.]
[The swap configured on the system is insufficient.]	Warning (80% of required swap detected) or Informational (90% of required swap detected)	[Consider adding more swap space to the system.]

Acronyms and Abbreviations

API	Application Programming Interface
AS	Application Server
ASR	Automated Speech Recognition
BCCT	BroadWorks Common Communication Transport
BW	BroadWorks
CAP	Client Application Protocol
CDR	Call Detail Record
CLI	Command Line Interface
CNAM	Caller ID with NAMe
CPU	Central Processing Unit
DB	Database
DBS	Database Server
DN	Directory Number
DNS	Domain Name System
DSN	Database Store Name
DTD	Document Type Definition
FQDN	Fully Qualified Domain Name
FTP	File Transfer Protocol
HTTP	Hypertext Transfer Protocol
IMRN	IP Multimedia Routing Number
IN	International
IP	Internet Protocol
LDAP	Lightweight Directory Access Protocol
MAC	Media Access Control
MB	Megabyte
MIB	Management Information Base
MIME	Multipurpose Internet Mail Extensions
MS	Media Server
MSC	Mobile Switching Centre
MWI	Message Waiting Indicator or Indication
NAPTR	Naming Authority Pointer
NS	Network Server
NTP	Network Time Protocol
OCI	Open Client Interface
OID	Object Identifier
PBX	Private Branch Exchange
PUI	Public User Identity

SCC	Service Centralization and Continuity
SCR	Selective Call Rejection
SIP	Session Initiation Protocol
SMDI	Simplified Message Desk Interface
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SOAP	Simple Object Access Protocol
SQL	Structured Query Language
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
UID	Unique Identifier
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
XML	eXtensible Markup Language
XS	Execution Server
Xsi	Xtended Services Interface

Index

C

E

F

I

M

N

O

P

R

S

T

References

[1] Cisco Systems, Inc. 2020. *Network Server Performance Measurement Interface Specification*. Available from Cisco at *https://cisco.com*.

References to Feature Description Documents

[FR 217550] Cisco Systems, Inc. 2020. *Node License Management Feature Description*, *Release 21.0*. Available from Cisco at *https://cisco.com*.

[FR 213706] Cisco Systems, Inc. 2020. *Network Server Split Upgrade Support Feature Description*, *Release 21.0*.
Available from Cisco at *https://cisco.com*.

[FR 173615] Cisco Systems, Inc. 2020. *External Authentication for MS Active Directory Feature Description*, *Release 20.0*.
Available from Cisco at *https://cisco.com*.

[FR 2299] Cisco Systems, Inc. 2017. *Network Database Server Feature Description*, *Release 22.0*. Available from Cisco at *https://cisco.com*.

[FR 2300] Cisco Systems, Inc. 2017. *Generic Database Change Notification Feature Description*, *Release 22.0*.
Available from Cisco at *https://cisco.com*.

[FR 6517] Cisco Systems, Inc. 2017. *Java Heap Monitoring Feature Description*, *Release 22.0*. Available from Cisco at *https://cisco.com*.

[FR 10066] Cisco Systems, Inc. 2017. *Enhanced Call Log DB Switch from Database Server Feature Description*, *Release 22.0*.
Available from Cisco at *https://cisco.com*.

[FR 11798] Cisco Systems, Inc. 2019. *Network Server Route Advancing Restrictions and Blacklisting Feature Description*, *Release 23.0*.
Available from Cisco at *https://cisco.com*.

[FR 18485] Cisco Systems, Inc. 2020. *Hazelcast Connectivity Alarm Feature Description*, *Release 24.0*. Available from Cisco at *https://cisco.com*.