



CHAPTER 10

Monitoring Cisco Broadband Access Center

This chapter describes how you can monitor the central RDU servers and the DPE servers in a Cisco Broadband Access Center (Cisco BAC) deployment. It describes:

- [Logging Events, page 10-1](#)
- [Monitoring Servers Using SNMP, page 10-9](#)
- [Monitoring Server Status, page 10-15](#)

Logging Events

Logging of events is performed at the RDU and the DPE, and in some unique situations, DPE events are additionally logged at the RDU to give them higher visibility.

Log files are stored in their own log directories and can be examined by using any text processor. You can compress the files for easier e-mailing to the Cisco Technical Assistance Center or system integrators for troubleshooting and fault resolution.

You can also access the RDU and the DPE logs from the administrator user interface.

Log Levels and Structures

The log file structure, illustrated in [Example 10-1](#), includes:

- Domain Name—This is the name of the computer generating the log files.
- Date and Time—This is the date on which a message is logged. This information also identifies the applicable time zone.
- Facility—This identifies the system, which (in this case) is Cisco BAC.
- Sub-facility—This identifies the Cisco BAC subsystem or component.

- **Severity Level**—The logging system defines seven levels of severity (as described in [Table 10-1](#)) that are used to identify the urgency with which you might want to address log issues. The process of configuring these severity levels is described in [Configuring Severity Levels, page 10-3](#).

Table 10-1 Severity Levels

Log Level	Description
0-Emergency	System unstable. Sets the logging function to save all emergency messages.
1-Alert	Immediate action needed. Sets the logging function to save all activities that need immediate action and those of a more severe nature.
2-Critical	Critical conditions exist. Sets the logging function to save all error messages and those of a more severe nature.
3-Error	Error conditions exist. Sets the logging function to save all error messages and those of a more severe nature.
4-Warning	Warning conditions exist. Sets the logging function to save all warning messages and those of a more severe nature.
5-Notification	A normal, but significant, condition exists. Sets the logging function to save all notification messages and those of a more severe nature.
6-Information	Informational messages. Sets the logging function to save all logging messages available.
Note	Another level known as 7-Debug is used exclusively by Cisco for debugging purposes. Do not use this level except at the direction of the Cisco Technical Assistance Center.

- **Msg ID**—This is a unique identifier for the message text.
- **Message**—This is the actual log message.

Example 10-1 Sample Log File

Domain Name	Data and Time	Facility	Sub-facility	Severity Level	Msg ID	Message
bac.example.com:	2007 9 6 03:06:11 EST:	%BAC-	RDU-	5	0236:	Broadband Access Center Regional Distribution Unit starting up
bac.example.com:	2007 9 6 03:06:15 EST:	%BAC-	RDU-	5	0566:	Initialized API defaults
bac.example.com:	2007 9 6 03:06:15 EST:	%BAC-	RDU-	5	0567:	Initialized Network Registrar defaults
bac.example.com:	2007 9 6 03:06:15 EST:	%BAC-	RDU-	5	0568:	Initialized Server defaults
bac.example.com:	2007 9 6 03:06:18 EST:	%BAC-	RDU-	5	0570:	Initialized DOCSIS defaults
bac.example.com:	2007 9 6 03:06:18 EST:	%BAC-	RDU-	5	0571:	Initialized Computer defaults
bac.example.com:	2007 9 6 03:06:19 EST:	%BAC-	RDU-	5	0573:	Initialized CableHome WAN-MAN defaults
bac.example.com:	2007 9 6 03:06:19 EST:	%BAC-	RDU-	5	0572:	Initialized PacketCable defaults
bac.example.com:	2007 9 6 03:06:19 EST:	%BAC-	RDU-	5	0569:	Created default admin user

Example 10-1 Sample Log File (continued)

Domain Name	Data and Time	Facility	Sub-facility	Severity Level	Msg ID	Message
bac.example.com:	2007 9 6 03:06:20 EST:	%BAC-	RDU-	5	0575:	Database initialization completed in [471] msec
bac.example.com:	2007 9 6 03:06:25 EST:	%BAC-	RDU-	3	0015:	Unable to locate manifest file
bac.example.com:	2007 9 6 03:06:28 EST:	%BAC-	RDU-	3	0280:	Command error

Configuring Severity Levels

You can configure the severity levels of logging for both the RDU and the DPE to suit your specific requirements. For example, the severity level for the RDU could be set to Warning, and the level for the DPE could be set to Alert.

Log messages are written based on certain events taking place. Whenever an event takes place, the appropriate log message and severity level are assigned and, if that level is less than or equal to the configured level, the message is written to the log. The message is not written to the log if the level is higher than the configured value.

For example, assume that the log level is set to 4-Warning. All events generating messages with a log level of 4 or less are written into the log file. If the log level is set to 6-Information, the log file will receive all messages. Consequently, configuring a higher log level results in a larger log file size.

**Note**

The KDC is not considered in this log file.

To configure the severity level on the DPE, use the **log level** command from the DPE command line. For detailed information, see the *Cisco Broadband Access Center DPE CLI Reference 4.2*.

To configure the log level tool on the RDU, see [Using the RDU Log Level Tool, page 10-4](#).

Rotating Log Files

All log files are numbered and rolled over based on a configured maximum file size. The default maximum file size is 25 MB. (To configure the maximum file size from the application programming interface [API], use the *ServerDefaultsKeys.SERVER_LOG_MAXSIZE* property.) Once a log file touches the configured limit, the data is rolled over to another file. This file is renamed in the *XXX.N.log* format, where:

- *XXX*—Specifies the name of the log file.
- *N*—Specifies any value between 1 and 200.

**Note**

The RDU and DPE servers store up to 200 log files at a given time. For a list of log files in these servers, see subsequent sections.

For example, once *rdu.log* reaches the 25-MB limit, it is renamed as *rdu.1.log*. With every 25-MB increase in file size, the latest file is renamed as *rdu.2.log*, *rdu.3.log*, and so on. So, the *rdu.4.log* file will contain data more recent than *rdu.7.log*. The latest log information, however, is always stored in *rdu.log*.

RDU Logs

The RDU has two logs that it maintains in the *BPR_DATA/rdu/logs* directory:


- *rdu.log*—Records RDU processing according to the configured default severity level. (For instructions on setting the default log levels, see [Setting the RDU Log Level, page 10-6.](#))
- *audit.log*—Records high-level changes to the Cisco BAC configuration or functionality including the user who made the change.

When you enable logging of informational messages (6-Information), the RDU logs additional messages that expose batch-processing operations. These messages also contain information on elapsed time and rate.

Viewing the *rdu.log* File

You can use any text processor to view the *rdu.log* file. In addition, you can view the log file from the administrator user interface.

To view the file:

-
- Step 1** Choose the RDU tab under **Servers**.
The View Regional Distribution Unit Details page appears.
- Step 2** Click the View Details icon () corresponding to RDU Log File.
The View Log File Contents page appears, displaying data from *rdu.log*.
-

Viewing the *audit.log* File

You can use any text processor to view the *audit.log* file. In addition, you can view the log file from the administrator user interface.

To view the file:

-
- Step 1** Choose the RDU tab under **Servers**.
The View Regional Distribution Unit Details page appears.
- Step 2** Click the View Details icon corresponding to Audit Log File.
The View Log File Contents page appears, displaying data from *audit.log*.
-

Using the RDU Log Level Tool

Use the RDU log level tool to change the current log level of the RDU from the command line, using the **setLogLevel.sh** command. This tool resides in the *BPR_HOME/rdu/bin* directory.

Table 10-2 identifies the available severity levels and the types of messages written to the log file when enabled.

Table 10-2 Logging Levels

Log Level	Description
0-Emergency	System unstable. Sets the logging function to save all emergency messages.
1-Alert	Immediate action needed. Sets the logging function to save all activities that need immediate action and those of a more severe nature.
2-Critical	Critical conditions exist. Sets the logging function to save all error messages and those of a more severe nature
3-Error	Error conditions exist. Sets the logging function to save all error messages and those of a more severe nature.
4-Warning	Warning conditions exist. Sets the logging function to save all warning messages and those of a more severe nature.
5-Notification	A normal, but significant, condition exists. Sets the logging function to save all notification messages and those of a more severe nature.
6-Information	Informational messages. Sets the logging function to save all logging messages available.
Note	Another level known as 7-Debug is used exclusively by Cisco for debugging purposes. Do not use this level except at the direction of the Cisco TAC.

We recommend that you keep the RDU severity level at the Warning level to help maintain a steady operations state. The Information level is recommended to be used with caution if you need to maintain steady state performance during debug operations. You should exercise caution when running with the Information level because this creates a great number of log entries, which in itself can adversely impact performance.



Note

The RDU process has to be up to execute the log level tool. Also, you must be a privileged user to run this tool by using the **setLogLevel.sh** command.

Syntax Description

setLogLevel.sh *[-[0..6]* **[-help]** **[-show]** **[-default]** **[-debug]**

- *[-[0..6]*—Identifies the severity level to be used. For a list of available levels, see [Table 10-2](#).
- **-help**—Displays help for the tool.
- **-show**—Displays the current severity level set for the RDU server.
- **-default**—Sets the RDU to the installation default level 5 (notification).
- **-debug**— Sets an interactive mode to enable or disable tracing categories for the RDU server.



Note

You should only enable the debug settings that the Cisco support staff recommends.

You can also use this tool to perform these functions:

- [Setting the RDU Log Level, page 10-6](#)
- [Viewing the Current Log Level of RDU, page 10-6](#)

Setting the RDU Log Level

You can use this tool to change the logging level from one value to another value. The following example illustrates how to set the RDU logging level to the warning level, as indicated by the number 4 in the **setLogLevel.sh** command. The actual log level set is not important for the procedure; it can be interchanged as required.

The example described in this section assumes that the RDU server is up, the username for the RDU is **admin**, and the password is **changeme**.

To set the RDU logging level:

Step 1 Change directory to *BPR_HOME/rdu/bin*.

Step 2 Run the RDU log level tool using this command:

```
# setLogLevel.sh 4
```

This prompt appears:

```
Please type RDU username:
```

Step 3 Enter the RDU username. In this example, the default username (**admin**) is used.

```
Please type RDU username: admin
```

This prompt appears:

```
Please type RDU password:
```

Step 4 Enter the RDU password for the RDU. In this example, the default password (**changeme**) is used.

```
Please type RDU password: changeme
```

This message appears to notify you that the log level has been changed. In this example, the level was 5, for notification, and is now 4, for warning.

```
RDU Log level was changed from 5 (notification) to 4 (warning).
```

Viewing the Current Log Level of RDU

You can use this tool to view the RDU log and determine which logging level is configured before attempting to change the value.

The example described in this section assumes that the:

- RDU server is up.
- Username for the RDU is **admin**.
- Password is **changeme**.

To view the current logging level of the RDU:

-
- Step 1** Change directory to *BPR_HOME/rdu/bin*.
- Step 2** Run this command:
- ```
setLogLevel.sh -show
```
- This prompt appears:
- Please type RDU username:
- Step 3** Enter the RDU username (**admin**) and press **Enter**.
- Please type RDU username: **admin**
- This prompt appears:
- Please type RDU password:
- Step 4** Enter the RDU password (**changeme**) and press **Enter**.
- Please type RDU password: **changeme**
- This message appears:
- The logging is currently set at level: 4 (warning)  
All tracing is currently disabled.
- 

## DPE Log

The DPE maintains a *dpe.log* file in the *BPR\_DATA/dpe/logs* directory. The file contains records of all events having the configured default level. In situations where the DPE undergoes catastrophic failure, such as engaging in a series of system crashes, the catastrophic errors are also logged into the *rdu.log* file.

The *SNMPService.logyyy.log* log file is used by the DPE, when PacketCable is enabled on the DPE server, to provide detailed debugging information. You use the **service packetcable 1..1 show snmp log** command from the DPE command-line interface (CLI) to view this file, which resides in the *BPR\_DATA/dpe/logs* directory. For PacketCable command usage, see the *Cisco Broadband Access Center DPE CLI Reference 4.2*.



### Note

PacketCable logging messages are sent to the *dpe.log* file and the detailed SNMP debugging is sent to the *SNMPService.logyyy.log* file.

You can use any text viewer to view the *dpe.log* file. In addition, you can use the **show log** command from the DPE CLI. For additional information, see the *Cisco Broadband Access Center DPE CLI Reference 4.2*.

You can also view the DPE log file using the Cisco BAC administrator user interface.

To view the file:

- 
- Step 1** Choose **Servers > DPEs**.
  - Step 2** Click the link of the DPE whose log file you want to view.  
The View Device Provisioning Engines Details page appears.
- 

## Network Registrar Logs

Cisco BAC generates log messages from Cisco Network Registrar DHCP server extensions. The DHCP server log resides in the *cnr-install-path/name\_dhcp\_1\_log* directory; *cnr-install-path* is a variable and is specific to the value that you enter. The default location for the DHCP server log file is */var/nwreg2/local/logs/name\_dhcp\_1\_log*.

The log messages emitted via the DHCP server extensions are based on the extension trace level setting. You can set values (described in [Table 10-3](#)) at the trace level; the number you set makes that number the current setting of the **extension-trace-level** attribute for all extensions.

**Table 10-3** DHCP Server Extension Trace Levels

| Level | Description                                                                                                                                                   |
|-------|---------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 0     | Logs error and warning conditions. Sets the extensions to emit all error and warning messages and those of a more severe nature.                              |
| 1     | Logs server interactions, which include configuration instructions obtained from the DPE and configuration generation requests that are forwarded to the RDU. |
| 2     | Logs processing details, which include individual configuration commands and attribute values forwarded in instruction generation requests.                   |
| 3     | Logs internal processing for extensions debugging, which includes hexadecimal dumps of messages.                                                              |
| 4     | Logs debugging of extension background operations, which include polling of DPE status.                                                                       |

You can change the extension trace level by using the Network Registrar web UI. To change the level:

- 
- Step 1** Open the Network Registrar local web UI.
  - Step 2** From the menu, click **DHCP**, then **DHCP Server**.
  - Step 3** Click the Local DHCP Server link.
  - Step 4** On the Edit DHCP Server page, expand the Extensions attribute category.
  - Step 5** Set the **extension-trace-level** value, then click **Modify Server**.
  - Step 6** Reload the DHCP server.
- 



**Note** For detailed information on logging performed by the DHCP server, see the *User Guide for Cisco Network Registrar 7.2*.

---



# Monitoring Servers Using SNMP

Cisco BAC supports management of servers via SNMP. Specifically, an SNMP-based management system can be used to monitor Cisco BAC server state, license utilization information, server connections, and server-specific statistics.

## SNMP Agent

Cisco BAC provides basic SNMP v2-based monitoring of the RDU and DPE servers. The Cisco BAC SNMP agents support SNMP informs and traps, collectively called notifications. You can configure the SNMP agent on the DPE using `snmp-server` CLI commands, and on the RDU using the SNMP configuration command-line tool.

For additional information on the SNMP configuration command-line tool, see [Using the `snmpAgentCfgUtil.sh` Tool](#), page 10-10. For additional information on the DPE CLI, see the *Cisco Broadband Access Center DPE CLI Reference 4.2*.

### MIB Support

Cisco BAC supports several different MIBs. [Table 10-4](#) summarizes MIB support for each Cisco BAC component.

**Table 10-4** Cisco BAC-Supported MIBs

| Component | MIBs Supported        |
|-----------|-----------------------|
| DPE       | CISCO-BACC-SERVER-MIB |
|           | CISCO-BACC-DPE-MIB    |
| RDU       | CISCO-BACC-SERVER-MIB |
|           | CISCO-BACC-RDU-MIB    |

The SNMP agent supports the CISCO-BACC-SERVER-MIB. This MIB defines the managed objects that are common to all servers on Cisco BAC. This MIB supports the monitoring of multiple Cisco BAC servers when they are installed on the same device. The `ciscoBaccServerStateChanged` notification is generated every time a server state change occurs.

The RDU SNMP agent supports the CISCO-BACC-RDU-MIB, which defines managed objects for the RDU. This MIB defines statistics related to the state of the RDU and the statistics on the communication interface between the RDU and DPE and between the RDU and Network Registrar.

The SNMP agent generates a `cnaHealthNotif` trap that announces that the RDU server has started, shut down, or failed, or there is a change in the exit status.

The DPE SNMP agent supports the CISCO-BACC-DPE-MIB, which defines managed objects for the components installed on a DPE. The DPE manages local caching of device configurations and configuration files used by all supported devices. This MIB provides some basic DPE configuration and statistics information, including entries for TFTP and ToD servers.

The SNMP agent also supports the CISCO-NMS-APPL-HEALTH-MIB, which defines the Cisco NMS application health status notifications and related objects. These notifications are sent to the OSS/NMS to inform them about the NMS application status, including: started, stopped, failed, busy, or any abnormal exit of applications. The default MIB is MIB-II.

**Note**

For a description of all objects, see the corresponding MIBs files in the *BPR\_HOME/rdu/mibs* directory.

## Using the `snmpAgentCfgUtil.sh` Tool

You can use the `snmpAgentCfgUtil.sh` tool to manage the SNMP agent installed on a Solaris computer. Using this tool, which resides in the *BPR\_HOME/snmp/bin* directory, you can add (or remove) your host to a list of other hosts that receive SNMP notifications, and start and stop the SNMP agent process. This tool should be run from the local directory.

**Note**

The default port number of an SNMP agent running on a Solaris computer is 8001.

You can use the RDU SNMP agent for:

- [Adding a Host, page 10-10](#)
- [Deleting a Host, page 10-11](#)
- [Adding an SNMP Agent Community, page 10-11](#)
- [Deleting an SNMP Agent Community, page 10-12](#)
- [Starting the SNMP Agent, page 10-12](#)
- [Stopping the SNMP Agent, page 10-13](#)
- [Configuring an SNMP Agent Listening Port, page 10-13](#)
- [Changing the SNMP Agent Location, page 10-13](#)
- [Setting Up SNMP Contacts, page 10-14](#)
- [Displaying SNMP Agent Settings, page 10-14](#)
- [Specifying SNMP Notification Types, page 10-15](#)

## Adding a Host

You use this command to add the host address to the list of hosts that receive SNMP notifications from the SNMP agent.

### Syntax Description

`snmpAgentCfgUtil.sh add host ip-addr community community [udp-port port]`

- *ip-addr*—Specifies the IP address of the host to which notifications are sent.
- *community*—Specifies the community (read or write) to be used while sending SNMP notifications.
- *port*—Identifies the UDP port used for sending the SNMP notifications.

### Examples

```
./snmpAgentCfgUtil.sh add host 10.10.10.5 community trapCommunity udp-port 162
OK
Please restart [stop and start] SNMP agent.
```



**Note** The changes that you introduce through this command do not take effect until you restart the SNMP agent by using the `/etc/init.d/bprAgent restart snmpAgent` command. For detailed information, see [Cisco BAC Process Watchdog, page 9-1](#).

## Deleting a Host

You use this command to remove a host from the list of those receiving SNMP notifications from the SNMP agent.

### Syntax Description

`snmpAgentCfgUtil.sh delete host ip-addr`

*ip-addr*—Specifies the IP address of the host that you want to delete from the list of hosts.

### Examples

```
./snmpAgentCfgUtil.sh delete host 10.10.10.5
OK
Please restart [stop and start] SNMP agent.
```



**Note** The changes that you introduce through this command do not take effect until you restart the SNMP agent by using the `/etc/init.d/bprAgent restart snmpAgent` command. For detailed information, see [Cisco BAC Process Watchdog, page 9-1](#).

## Adding an SNMP Agent Community

You use this command to add an SNMP community string to allow access to the SNMP agent.

### Syntax Description

`snmpAgentCfgUtil.sh add community string [ro | rw]`

- *string*—Identifies the SNMP community.
- **ro**—Assigns a read-only (**ro**) community string. Only *get* requests (queries) can be performed. The *ro* community string allows *get* requests, but no *set* operations. The NMS and the managed device must reference the same community string.
- **rw**—Assigns a read-write (**rw**) community string. SNMP applications require read-write access for *set* operations. The **rw** community string enables write access to OID values.



**Note** The default **ro** and **rw** community strings are `baccread` and `baccwrite`, respectively. We recommend that you change these values before deploying Cisco BAC.

**Examples**

```
./snmpAgentCfgUtil.sh add community fsda54 ro
OK
Please restart [stop and start] SNMP agent.
```



**Note** The changes that you introduce through this command do not take effect until you restart the SNMP agent by using the `/etc/init.d/bprAgent restart snmpAgent` command. For detailed information, see [Cisco BAC Process Watchdog, page 9-1](#).

**Deleting an SNMP Agent Community**

You use this command to delete an SNMP community string to prevent access to the SNMP agent.

**Syntax Description**

`snmpAgentCfgUtil.sh delete community string [ro | rw]`

- *string*—Identifies the SNMP community.
- **ro**—Identifies the specified community as a read-only one.
- **rw**—Identifies the specified community as a read-write one.



**Note** See [Adding an SNMP Agent Community, page 10-11](#), for additional information on the **ro** and **rw** community strings.

**Examples**

```
./snmpAgentCfgUtil.sh delete community fsda54 ro
OK
Please restart [stop and start] SNMP agent.
```



**Note** The changes that you introduce through this command do not take effect until you restart the SNMP agent by using the `/etc/init.d/bprAgent restart snmpAgent` command. For detailed information, see [Cisco BAC Process Watchdog, page 9-1](#).

**Starting the SNMP Agent**

You use this command to start the SNMP agent process on a Solaris computer on which Cisco BAC is installed.



**Note** You can also start the SNMP agent by invoking the Cisco BAC process watchdog using the `/etc/init.d/bprAgent start snmpAgent` command. For more information, see [Using the Cisco BAC Process Watchdog from the Command Line, page 9-2](#).

**Examples**

```
./snmpAgentCfgUtil.sh start
Process snmpAgent has been started
```

## Stopping the SNMP Agent

You use this command to stop the SNMP agent process on a Solaris computer on which Cisco BAC is installed.



### Note

You can also stop the SNMP agent by invoking the Cisco BAC process watchdog using the `/etc/init.d/bprAgent stop snmpAgent` command. For more information, see [Using the Cisco BAC Process Watchdog from the Command Line, page 9-2](#).

### Examples

```
./snmpAgentCfgUtil.sh stop
Process snmpAgent has stopped
```

## Configuring an SNMP Agent Listening Port

You use this command to specify the port number that the SNMP agent will listen to. The default port number used by RDU SNMP agent is 8001.

### Syntax Description

```
snmpAgentCfgUtil.sh udp-port port
```

*port* identifies the port number that the SNMP agent will listen to.

### Examples

```
./snmpAgentCfgUtil.sh udp-port 8001
OK
Please restart [stop and start] SNMP agent.
```



### Note

The changes that you introduce through this command do not take effect until you restart the SNMP agent by using the `/etc/init.d/bprAgent restart snmpAgent` command. For detailed information, see [Cisco BAC Process Watchdog, page 9-1](#).

## Changing the SNMP Agent Location

You use this command to enter a string of text that indicates the location of the device running the SNMP agent. This could, for example, be used to identify the physical location of the device. You can enter any character string that is fewer than 255 characters.

### Syntax Description

```
snmpAgentCfgUtil.sh location location
```

*location* is the character string identifying the agent's location.

### Examples

In this example, the physical location of the SNMP agent is in an equipment rack identified as rack 5D:

```
./snmpAgentCfgUtil.sh location "equipmentrack5D"
OK
Please restart [stop and start] SNMP agent.
```



**Note** The changes that you introduce through this command do not take effect until you restart the SNMP agent by using the `/etc/init.d/bprAgent restart snmpAgent` command. For detailed information, see [Cisco BAC Process Watchdog, page 9-1](#).

## Setting Up SNMP Contacts

You can use this command to enter a string of text that identifies the contact person for the SNMP agent, together with information on how to contact this person. This could, for example, be used to identify a specific person including that person's telephone number. You can enter any character string that is fewer than 255 characters.

### Syntax Description

`snmpAgentCfgUtil.sh contact contact-info`

*contact-info* is the character string identifying the individual to contact concerning the SNMP agent.

### Examples

In this example, the contact name is Terry and the telephone extension is 1234:

```
./snmpAgentCfgUtil.sh contact "Terry-ext1234"
OK
Please restart [stop and start] SNMP agent.
```



**Note** The changes that you introduce through this command do not take effect until you restart the SNMP agent by using the `/etc/init.d/bprAgent restart snmpAgent` command. For detailed information, see [Cisco BAC Process Watchdog, page 9-1](#).

## Displaying SNMP Agent Settings

You use this command to display all current SNMP settings.

### Examples

```
./snmpAgentCfgUtil.sh show
Location : equipmenttrack5D
Contact : Terry-ext1234
Port Number : 8001
Notification Type : trap
Notification Recipient Table :
 [Host IP address, Community, UDP Port]
 [10.10.10.5 , trapCommunity , 162]
Access Control Table :
 Read Only Communities
 baccread
 Read Write Communities
 baccwrite
```

## Specifying SNMP Notification Types

You use this command to specify the types of notifications (traps or informs) that will be sent from the SNMP agent. By default, traps are sent, though you can set the agent to send SNMP informs instead.



### Note

For the SNMP trap feature to work, you must enable the notification flag. In other words, the value for the MIB variable `0cbsNotifEnableFlags` (OID = `.1.3.6.1.4.1.9.9.349.1.1.1.5.1`) must be set to 1.

### Syntax Description

**snmpAgentCfgUtil.sh inform [retries timeout] | trap**

Where the parameter is the backoff timeout between retries.

### Examples

```
./snmpAgentCfgUtil.sh inform retries 3 timeout 1000
OK
Please restart [stop and start] SNMP agent.
```



### Note

The changes that you introduce through this command do not take effect until you restart the SNMP agent by using the `/etc/init.d/bprAgent restart snmpAgent` command. For detailed information, see [Cisco BAC Process Watchdog, page 9-1](#).

Use the `snmpAgentCfgUtil.sh show` command to verify your configuration settings.

```
./snmpAgentCfgUtil.sh show
Location : equipmentrack5D
Contact : Terry-ext1234
Port Number : 8001
Notification Type : inform
Notification Retries : 3
Notification Timeout : 1000
Notification Recipient Table :
 [Host IP address, Community, UDP Port]
 [10.10.10.5 , trapCommunity , 162]
Access Control Table :
 Read Only Communities
 baccread
 Read Write Communities
 baccwrite
```

## Monitoring Server Status

This section describes how you can monitor the performance of the RDU and DPE servers in a Cisco BAC deployment. These servers are the central RDU server and the DPE servers.

You can check server statistics from the:

- Administrator user interface
- DPE CLI
- RDU and DPE log files using the administrator user interface or the DPE CLI.

## Using the Administrator User Interface

To view server statistics available on the administrator user interface:

1. On the Primary Navigation Bar, click the **Server** tab.  
The Secondary Navigation Bar displays your options: DPEs, NRs, Provisioning Group, RDU.
2. Click the:
  - DPEs tab to monitor all DPEs currently registered in the Cisco BAC database.
  - RDU tab to display RDU status and statistics.

If you clicked:

- DPEs—The Manage Device Provisioning Engine page appears.

Each DPE name on this page is a link to another page that shows the details for that DPE. Click this link to display the details page.

- RDU—The View Regional Distribution Unit Details page appears.

## Using the DPE CLI

To monitor the status of the DPE server, run the **show dpe** command to check if the DPE is running and displays the state of the process and, if running, its operational statistics. See [Example 10-2](#).



### Note

---

This command does not indicate if the DPE is running successfully, only that the process itself is currently executing. However, when the DPE is running, you can use statistics that this command prints to determine if the DPE is successfully servicing requests.

---

### Example 10-2 show dpe Output

This result occurs when the DPE is running.

```
dpe# show dpe
BAC Agent is running
Process dpe is running
Version BAC 4.2 (SOL_CBAC4_0_L_000000000000).
Caching 1 device configs and 1 external files.
0 sessions succeed and 0 sessions failed.
0 file requests succeed and 0 file requests failed.
0 immediate proxy operations received: 0 succeed, and 0 failed.
Connection status is Ready.
Running for 4 hours 30 mins 16 secs.
```

This result occurs when the DPE is not running.

```
dpe_host# show dpe
BAC Agent is running
Process dpe is not running
```



### Note

---

For more information, see the *Cisco Broadband Access Center DPE CLI Reference 4.2*.

---