
# 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 (BAC) deployment.

This chapter includes the following sections:



# Syslog Alert Messages

Cisco BAC generates alerts through the syslog service. Syslog is a client-server protocol that manages the logging of information. Cisco BAC syslog alerts are not a logging service; they provide a notification that a problem exists, but do not necessarily define the specific cause of the problem. You might find this information in the appropriate Cisco BAC log files.

## Message Format

When Cisco BAC generates an alert message, the format is:

*XXX-#-####: Message*

- *XXX*—Identifies the facility code, which can include:
  - RDU (regional distribution unit).
  - DPE (device provisioning engine).
  - AGENT (Cisco BAC process watchdog).
- *#*—Identifies the severity level in use. The three levels of alerts are:
  - 1, which is alert.
  - 3, which is error.
  - 6, which identifies informational messages.
- *###*—Identifies the numeric error code as described in the following sections.

- *Message*—Provides the alert text or message.

# RDU Alerts

Table 11-1 identifies the RDU alerts.

***Table 11-1 RDU Alerts***

| Alert | Description |
|---|---|
| RDU-1-101: RDU ran out of disk space | Indicates that the storage partition that the RDU server uses ran out of space. After encountering this error, the RDU attempts to restart automatically, but will typically encounter the same error again until more storage space is available.<br>See Cisco BAC Support Tools and Advanced Concepts, page 20-1, for additional information on upgrading the disk. |
| RDU-1-103: RDU ran out of memory | Indicates that the RDU ran out of memory. After encountering this error, the RDU server restarts automatically. |
| RDU-1-111: Evaluation key for technology *[technology_name]* expired | Appears if an evaluation key for the technology specified expires. You must contact Cisco sales or TAC for a new license key. |
| RDU-1-115: You have used *[percent]percent* of available *[technology_name]* licenses | Identifies the quantity of licences used (in percentage) out of the total number of allowable licenses. Appears when you reach 80% of the license capacity. |
| BPR-RDU-4-1140: DNS took *X* seconds for lookup of address [10.0.0.1/test.com]; Check DNS configuration and health of servers | Indicates that Cisco BAC performance may be slow due to delayed response from the DNS. The alert is generated whenever IP Address look-up takes more than 60 seconds. |
| **Note** Whenever an RDU syslog alert is sent, additional details (if any) can be found in log file <BPR_DATA>/rdu/logs/rdu.log. | |

# DPE Alerts

Whenever a DPE syslog alert is sent, you can find additional details in the DPE logs.

You can use the **show log** command to access the DPE logs. See *Cisco Broadband Access Center 3.8 DPE CLI Reference,* for additional information.

Some DPE errors are also propagated to the RDU server log files. You can find these in the <BPR_DATA>/rdu/logs/rdu.log file.

Table 11-2 identifies the DPE alerts.

***Table 11-2 DPE Alerts***

| Alert | Description |
|---|---|
| DPE-1-102: DPE ran out of disk space | The storage partition that the DPE server uses ran out of space. You have three options:<br>**a.** Clear out any excess support bundles that may reside on the disk.<br>You can do this by moving those support bundles to another machine and then running the **clear bundles** command from the DPE CLI.<br>**b.** Run the **clear logs** command from the DPE CLI to clear more disk space.<br>**c.** As a last resort, run the **clear cache** command from the DPE CLI to remove any cache files and force the DPE to resynchronize with the RDU server. |
| DPE-1-104: DPE ran out of memory | The DPE process ran out of memory. After encountering this error condition, the DPE restarts automatically.<br>Determine how many device configurations are on the DPE; the larger the number of device configurations, the more memory is used.<br>To reduce device configurations, limit the number of devices in the provisioning groups that the DPE serves. |
| DPE-1-109: Failed to connect to RDU<br><br>Clear:<br>DPE-1-123: Successfully connected to RDU | The RDU cannot be contacted. You must:<br>**a.** Verify that the DPE network is configured and connected correctly.<br>**b.** Check that the DPE is configured to connect to the proper RDU, and that the connecting port is configured properly by using the **dpe rdu-server** command.<br>**c.** Check that the RDU process is running on the correct server and listening on the correct port. The DPE attempts to reconnect to the RDU process every few seconds until a connection is established. |

*Table 11-2 DPE Alerts (continued)*

| Alert | Description |
|---|---|
| DPE-1-125: Configured extension script file is missing<br><br>Clear:<br>DPE-1-126: Configured extension script file is available | The configured script file is not available in the DPE cache. This alert will be fired only once per script.<br><br>This error cannot be manually cleared. Once the error is cleared, a clear alert is fired. |
| DPE-1-127: Configured extension script file failed for the device<br><br>Clear:<br>DPE-1-128: Configured extension script file executed for the device | The configured script for a device has failed. This alert will be fired only once for a script failure per device.<br><br>This error cannot be manually cleared. Once the error is cleared, a clear alert is fired. |

# Watchdog Agent Alerts

Whenever the watchdog process sends a syslog alert, you can find error details (if any) in the <BPR_DATA>/agent/logs/agent_console.log file and the log files corresponding to the specific component mentioned in the alert (if any).

For example, if you receive an alert similar to `The rdu unexpectedly terminated`, you would check the RDU server log file (<BPR_DATA>/rdu/logs/rdu.log) for additional information. Table 11-3 identifies the watchdog agent alerts.

*Table 11-3 Watchdog Agent Alerts*

| Alert | Description |
|---|---|
| AGENT-3-9001: Failed to start the *component* | Indicates that the watchdog has failed to start the specified component. |
| AGENT-3-9002: The *component* unexpectedly terminated | Indicates that the specified component, that the agent process monitors, unexpectedly failed. |
| AGENT-3-9003: Failed to stop the *component* | Indicates that a component did not stop when the watchdog agent attempted to stop it. |
| AGENT-6-9004: The *component* has started | Is generated any time the watchdog agent successfully starts a component. This message is for informational purposes only. |
| AGENT-6-9005: The *component* has stopped | Is generated any time the watchdog agent a successfully stops a component. This message is for informational purposes only. |

The *component* variable presented in the watchdog agent alerts list shown in Table 11-3 represents any of these component values:

- rdu
- dpe

- tomcat
- cli
- snmpAgent

## Access Registrar Extension Point Alerts

Whenever a Cisco BAC Access Registrar extension point syslog alert is sent, you can find additional details in the Access Registrar log file in *<AR_HOME>/logs/name_radius_1_log*.

***Table 11-4 Access Registrar Extension Point Alerts***

| Alert | Description |
|---|---|
| **Error**:<br>Auth HTTP Adapter: Failed to initialize Background thread pool and Request queue, due to *Exception_message*<br>**Clear**:<br>Auth HTTP Adapter: Background thread pool and Request queue initialized successfully. | The Access Registrar failed to initialize the background threads and queue in the extension point service. |
| **Error**:<br>Auth HTTP Adapter: Failed to initialize Http connections, due to *Exception_message*<br>**Clear**:<br>Auth HTTP Adapter: Http connections initialized successfully. | The Access Registrar failed to initialize the HTTP connection manager in the extension point service. |
| **Error:**<br>Auth HTTP Adapter: Extension point unable to find a usable Auth Service.<br>**Clear**:<br>Auth HTTP Adapter: HTTP message POST successful. | The alert message will be sent if the Extension point could not find a usable DPE Auth service. |

# Monitoring Servers by Using SNMP

Cisco BAC supports management of servers using 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

The Cisco BAC SNMP agents support SNMP informs and traps, collectively called as notifications hereafter. You can configure the SNMP agent on the DPE by using snmp-server CLI commands, and on the RDU by using the **snmpAgentCfgutil.sh** tool.

See Using the snmpAgentCfgUtil.sh Tool, page 11-6, for additional information on the SNMP configuration command line tool, and the *Cisco Broadband Access Center 3.8 DPE CLI Reference,* for additional information on the DPE CLI.

## MIB Support

Cisco BAC supports several different MIBs. These include:

- CISCO-BACC-DPE-MIB
- CISCO-BACC-RDU-MIB
- CISCO-BACC-SERVER-MIB

Table 11-5 summarizes the MIB support in Cisco BAC:

***Table 11-5 Cisco BAC-Supported MIBs***

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

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.

The DPE SNMP agent supports the CISCO-BACC-DPE-MIB, which defines managed objects for the DPE. This MIB provides some basic DPE configuration and statistics information.

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.

**Note** For a description of all objects, refer to the corresponding MIB files under the *<BPR_HOME>/rdu/mibs* directory.

# Using the snmpAgentCfgUtil.sh Tool

You can use the **snmpAgentCfgUtil.sh** tool to manage the SNMP agent.

By using this tool, which is located 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.

**Note** The default port number of an SNMP agent is 8001.

You can use the **snmpAgentCfgUtil.sh** tool for:



## 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** *host-addr* **community** *community* [**udp-port** *port*]

- *host-addr*—Specifies the IP address of the host that you want to add to the list of hosts.
- *community*—Specifies the community (read or write) to use while sending SNMP notifications.
- *port*—Identifies the UDP port used for sending the SNMP notifications.

**Examples**

```
# ./snmpAgentCfgUtil.sh add host test.cisco.com 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** *host-addr*

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

**Examples**

```
# ./snmpAgentCfgUtil.sh delete host test.cisco.com
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 restrict access to the SNMP agent. The SNMP community name is used as a shared secret, with SNMP managers accessing the Cisco BAC 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 network management system 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 object identifier (OID) values.

**Note** The default **ro** and **rw** community strings are `bacread` and `bacwrite`, respectively. Cisco recommends that you change these values before deploying Cisco BAC. To change them, add new community names and delete the default ones.

**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**—Assigns a read-only (**ro**) community string
- **rw**—Assigns a read-write (**rw**) community string

**Note** For additional information on the **ro** and **rw** community strings, see Adding an SNMP Agent Community, page 11-8.

**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 any computer on which Cisco BAC is already installed.

**Note** You can also start the SNMP agent by invoking the Cisco BAC watchdog process agent by using the **/etc/init.d/bprAgent start snmpAgent** command. For more information, see Using 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 any computer on which Cisco BAC is already installed.

**Note** You can also stop the SNMP agent by invoking the Cisco BAC watchdog process agent by using the **/etc/init.d/bprAgent stop snmpAgent** command. For more information, see Using 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 which the SNMP agent will listen on. The default port number that the RDU SNMP agent uses is 8001.

**Syntax Description**

**snmpAgentCfgUtil.sh udp-port** *port*

*port*— Identifies the port number which the SNMP agent will listen on.

**Examples**

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

## Changing the SNMP Agent Location

You use this command to enter a string of text that you use to indicate the location of the device running the SNMP agent. For example, you could use this string to identify the physical location of the device. You can enter any string up to 255 characters long.

**Syntax Description**

**snmpAgentCfgUtil.sh location** *location*

*location*—Specifies the character string identifying the agents location.

**Examples**

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

```
# snmpAgentCfgUtil.sh location "equipment rack 5D"
```

## Setting Up SNMP Contacts

You use this command to enter a string of text that you use to identify the contact person for the SNMP agent, together with information on how to contact this person. For example, you could use this string to identify a specific person including that person's telephone number. You can enter any string up to 255 characters long.

**Syntax Description**

**snmpAgentCfgUtil.sh contact** *contact-info*

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

**Examples** In this example, the contact name is *Ace Duffy* and the telephone extension is *1234*:

```
# ./snmpAgentCfgUtil.sh contact "Ace Duffy - ext 1234"
```

## Displaying SNMP Agent Settings

You use this command to display all current SNMP settings.

**Syntax Description**

```
snmpAgentCfgUtil.sh show
```

**Examples**

```
# ./snmpAgentCfgUtil.sh show
Location                      : Washington_1
Contact                       : John
Port Number                   : 8001
Notification Type             : trap
Notification Recipient Table  :
        [ Host IP address, Community, UDP Port ]
       [ 10.10.10.1, public, 162 ]
Access Control Table          :
        Read Only Communities
                bacread
        Read Write Communities
                bacwrite
```

## Specifying SNMP Notification Types

You use this command to specify which types of notifications (traps or informs) the SNMP agent will send. By default, the agent sends traps; although you can set this 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 = .1.3.6.1.4.1.9.9.349.1.1.1.1.5.1) must be set to 1.

**Syntax Description**

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

Where the parameter is the back-off timeout between retries.

**Examples**

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

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

```
#  ./snmpAgentCfgUtil.sh show
Location                      : <unknown>
Contact                       : <unknown>
Port Number                   : 8001
Notification Type             : inform
Notification Retries          : 3
```

```
Notification Timeout          : 1000
Notification Recipient Table  :
        [ Host IP address, Community, UDP Port ]
Access Control Table          :
        Read Only Communities
                bacread
        Read Write Communities
                bacwrite
```

# 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:

**Step 1** On the Primary Navigation Bar, click the **Server** tab.

**Step 2** The Secondary Navigation Bar displays your options: DPEs, Provisioning Group, RDU.

Click the:

- **DPEs** tab to monitor all DPEs currently registered in the Cisco BAC database.
- **RDU** tab to display RDU status and statistics.

**Step 3** 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

You can run the **show dpe** command to view the status of the DPE server. 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 displays to determine if the DPE is successfully servicing requests.

You can use the **show run** command to view the current configuration settings on the DPE.

***Example 11-1 show dpe Output***

```
dpe# show dpe
```

```
BAC Agent is running
Process dpe is not running
```

This result occurs when the DPE is not running.

```
dpe# show dpe
BAC Agent is running
Process dpe is running

Broadband Access Center [BAC 3.8 <SOL_BAC_3_5_200081208_1446>].
Connected to RDU
Caching 10001 device configs and [3] files.
100 sessions succeeded and 12 sessions failed.
200 file requests succeeded and 3 file requests failed.
34 immediate device operations succeeded, and 0 failed.
12 home PG redirections succeeded, and 0 failed.
Using Signature key name [] with a vality of [3600].
Running for [12] days [20] hours [59] mins [5] secs.
```

This result occurs when the DPE is running.

### *Example 11-2 show run output*

```
dpe# show run
dpe service-auth xml-schema enable true
dpe shared-secret <value is set>
interface ip 10.86.147.122 pg-communication
log level 5-notification
no debug
service auth 1 address 127.0.0.1
service auth 1 enabled true
service auth 1 port 7551
service auth 1 ssl enabled false
service cwmp 1 client-auth digest
service cwmp 1 enabled true
service cwmp 1 port 7547
service cwmp 1 ssl cipher all-cipher-suites
service cwmp 1 ssl client-auth none
service cwmp 1 ssl enabled false
service cwmp 1 ssl keystore server-certs <value is set> <value is set>
service cwmp 2 client-auth digest
service cwmp 2 enabled false
service cwmp 2 port 7548
service cwmp 2 ssl cipher all-cipher-suites
service cwmp 2 ssl client-auth none
service cwmp 2 ssl enabled true
service cwmp 2 ssl keystore server-certs <value is set> <value is set>
service cwmp session timeout 60000
service cwmp-redirect 1 attempts 3
service cwmp-redirect 1 limit 20
service cwmp-redirect 1 lookup enabled true
service cwmp-redirect 1 respond enabled true
service cwmp-redirect 1 retry-after-timeout 60
service cwmp-redirect 1 status-period 5000
service cwmp-redirect 1 timeout 500
service http 1 client-auth digest
service http 1 enabled true
service http 1 port 7549
service http 1 ssl cipher all-cipher-suites
service http 1 ssl client-auth none
service http 1 ssl enabled false
service http 1 ssl keystore server-certs <value is set> <value is set>
service http 2 client-auth digest
```

```
service http 2 enabled false
service http 2 port 7550
service http 2 ssl cipher all-cipher-suites
service http 2 ssl client-auth none
service http 2 ssl enabled true
service http 2 ssl keystore server-certs <value is set> <value is set>
snmp-server community bacread ro
snmp-server community bacwrite rw
snmp-server contact <unknown>
snmp-server location <unknown>
snmp-server udp-port 8001
tacacs-server retries 2
tacacs-server timeout 5
```

**Note** For more information, see the *Cisco Broadband Access Center 3.8 DPE CLI Reference*.

# Monitoring Performance Statistics

Cisco BAC provides a rich set of statistics to aid in troubleshooting system performance. The statistics are available across different major components, including the RDU, the Provisioning API Command Engine, and device operations.

You can enable the collection of performance statistics from the administrator user interface or from the DPE CLI.

- To enable or disable performance statistics on the RDU, from the user interface, choose **Configuration > Defaults > System Defaults**.
  - To enable this feature, against Performance Statistics Collection, click the **Enabled** radio button.
  - To disable this feature, against Performance Statistics Collection, click the **Disabled** radio button.
- To enable or disable performance statistics on the DPE, from the DPE CLI in the enabled mode, enter **debug dpe statistics**. To disable performance statistics from the CLI, use the **no debug dpe statistics** command.

**Note** Before using any debug command, ensure that DPE debugging is enabled by running the **debug on** command. For more information, see the *Cisco Broadband Access Center 3.8 DPE CLI Reference*.

After you enable the performance statistics feature, you can choose to view performance statistics from the perfstat.log file or analyze the data by using the **runStatAnalyzer.sh** tool.

You can also view CWMP statistics specifically by using the administrator user interface. Choose **Servers > DPEs > Manage Device Provisioning Page > View Device Provisioning Engines Details.** (See Figure 16-7.)

For details on performance statistics collection, see:

- Understanding perfstat.log, page 11-15
- Using runStatAnalyzer.sh, page 11-15

# Understanding *perfstat.log*

You can monitor performance statistics by using the data recorded in the perfstat.log file, in which statistics data is logged at specific intervals; this time interval is 5 minutes. The perfstat.log file resides in separate directories for the RDU *(<BPR_DATA>/rdu/logs/statistics*) and the DPE (<BPR_DATA>/dpe/logs/statistics).

Each *perfstat.log* file stores data for a minimum of one day and a maximum of 30 days. Since you can turn on and turn off the performance statistics feature, the logs may not represent data for consecutive days.

The *perfstat.log* file is renamed every day by using the *perfstat.N*.log format, where *N* is any value between 1 and 100. For example, *perfstat.100.log* will be the oldest log while *perfstat.1.log* will be the most recent renamed *perfstat.log* file.

**Note** The data is stored in comma-separated vector format. The format of each statistic is *yyyymmdd:hh:mm*, *component*, *interval-in-milliseconds*, *stat1-tag*, *stat1-value*, *stat2-tag*, *stat2-value*, … *Stat1-tag* and *stat1-value* specify the tag ID and the value of each statistic, respectively.

# Using *runStatAnalyzer.sh*

You can use Cisco BAC to analyze and provide a summary of performance statistics by using the **runStatAnalyzer.sh** tool. To analyze collected performance statistics, run the **runStatAnalyzer.sh** tool from the:

- <BPR_HOME>/rdu/bin directory for the RDU.
- <BPR_HOME>/dpe/bin directory for the DPE.

## Syntax Description

```
# runStatAnalyzer.sh [-d perfdata-dir] [-s start-time] [-e end-time] [-c component]
[-f output-format] [-help] [-help components] [-help statistics [component]]
```

- **perfdata-dir**—Specifies the directory from which performance statistics are analyzed. This is the *perfstatN.dat* file located in the following default directories:
  - <BPR_HOME>/rdu/logs/statistics for the RDU
  - <BPR_HOME>/dpe/logs/statistics for the DPE
- *start-time*—Specifies the time from which collected data is to be analyzed. By default, all collected statistics are reported. Use this time format to specify *start-time*: *yyyy-mm-dd:hh:mm*.
- *end-time*—Specifies the time until which data collected data is to be analyzed. By default, all collected statistics are reported. Use this time format to specify *end-time*: *yyyy-mm-dd:hh:mm*.

- *component*—Specifies the Cisco BAC component for which you want to analyze statistics. You can choose to specify all components (by using the **all** option) or specify from the following list of supported components:

| Component Option | Description | Applicable at | |
|---|---|---|---|
| | | RDU | DPE |
| **pace** | Provisioning API Command Engine | **P** | |
| **rdu** | Regional Distribution Unit | **P** | |
| ext | Extensions | **P** | |
| cwmp | CWMP Service | | **P** |
| httpfile | HTTP File Service | | **P** |
| proxyreq | Proxy Request Operations | **P** | **P** |
| leasequery | Lease Query | | **P** |
| Authservice | AUTH service | | **P** |
| cmhscr | CMHS Connection Request | **P** | |
| scriptableExt | Scriptable Extension | | **P** |
| moip | Multi-Instance Object Processing | | **P** |

**Note** By default, statistics are analyzed for all components.

- *output-format*—Specifies the format of the output you want, which could be:
  - **summary**—Provides output of the transaction rate summary. This is the default option.

**Note** The summarized transaction rate is calculated based on the 5-minute interval data recorded in *perfstat.log*.

  - **log**—Provides output similar to a log message.
- **-help**—Provides usage information on the **runStatAnalyzer.sh** tool.
- **-help components**—Provides information on the Cisco BAC component for which you can analyze statistics.
- **-help statistics** *component*—Provides information on the statistics that each Cisco BAC component returns. You can choose to view help for all components (by using the **all** option) or for individual components: **pace**, **rdu**, **ext**, **cwmp**, **httpfile**, **proxyreq**.

***Example 11-3 Log Output Through runStatAnalyzer.sh***

```
# runStatAnalyzer.sh -s 2006-04-11:12:59 -e 2006-04-11:13:09 -c pace -f log

2006-04-11:12:59 PACE statistics last 5 minutes- In Queue 0; Dropped 0; Dropped-Full Queue
0; Batches Received 0; Internal Batches Received 0; Succeed 0; Failed 0; Processed 0;
Processing avgTime 0 msec; Batch maxTime 0 msec; In Queue maxTime 0 msec; Processing
maxTime 0 msec; CRS Completed 0
2006-04-11:13:04 PACE statistics last 5 minutes- In Queue 0; Dropped 0; Dropped-Full Queue
0; Batches Received 0; Internal Batches Received 0; Succeed 0; Failed 0; Processed 0;
Processing avgTime 0 msec; Batch maxTime 0 msec; In Queue maxTime 0 msec; Processing
maxTime 0 msec; CRS Completed 0
```

```
2006-04-11:13:09 PACE statistics last 5 minutes- In Queue 0; Dropped 0; Dropped-Full Queue
0; Batches Received 0; Internal Batches Received 0; Succeed 0; Failed 0; Processed 0;
Processing avgTime 0 msec; Batch maxTime 0 msec; In Queue maxTime 0 msec; Processing
maxTime 0 msec; CRS Completed 0
```

**Note** The number of statistics available varies on the component specified.

***Example 11-4 Summary Output Through runStatAnalyzer.sh***

```
# runStatAnalyzer.sh -s 2006-04-11:12:59 -e 2006-04-11:13:29 -c pace -f summary

2006-04-11:13:04 PACE statistics last 5 minutes- In Queue 0; Dropped 0; Dropped-Full Queue
0; Batches Received 0; Internal Batches Received 0; Succeed 0; Failed 0; Processed 0;
Processing avgTime 0 msec; Batch maxTime 0 msec; In Queue maxTime 0 msec; Processing
maxTime 0 msec; CRS Completed 0
2006-04-11:13:29 PACE statistics last 30 minutes- In Queue 0; Dropped 0; Dropped-Full
Queue 0; Batches Received 0; Internal Batches Received 0; Succeed 0; Failed 0; Processed
0; Processing avgTime 0 msec; Batch maxTime 0 msec; In Queue maxTime 0 msec; Processing
maxTime 0 msec; CRS Completed 0
```

**Note** Summarized data is visible only if a complete set of data is available for the given interval. For example, the summary output of a 30-minute summarized interval appears only if there is 30 minutes worth of data. Based on the data available, the summarized time intervals are 5 minutes, 30 minutes, 60 minutes, 3 hours, 6 hours, 12 hours, 24 hours, 7 days, 14 days, 21 days, and 30 days.

# Traffic Profiling

Cisco BAC provides details about the traffic between the CPE and the DPE to provide visibility into flows that may be causing issues. This traffic profiling provides statistics on the following:

- Number of CWMP sessions handled
- Number of devices rejected
- Number of HTTP file requests handled
- Home Provisioning Group redirection status
- Traffic caused by chatty clients

The periodic statistics provides details, including the name of each Remote Procedure Call (RPC) and the specific types of Inform messages. The following RPC methods are monitored and reported:

- GetRPCMethods
- SetParameterValues
- GetParameterValues
- SetParameterAttributes
- GetParameterAttributes
- AddObject
- DeleteObject
- Download
- Reboot

- Inform
- TransferComplete
- AutonomousTransferComplete
- GetQueuedTransfers
- ScheduleInform
- SetVouchers
- GetOptions
- Upload
- FactoryReset
- GetAllQueuedTransfers
- Kicked
- RequestDownload

To enable or disable traffic statistics on the RDU, from the user interface, choose **Configuration > Defaults > System Defaults**.

- To enable this feature, against Performance Statistics Collection, click the **Enabled** radio button.
- To disable this feature, against Performance Statistics Collection, click the **Disabled** radio button.

To enable or disable traffic statistics on the DPE, from the DPE CLI in the enabled mode, enter **debug dpe statistics**. To disable traffic profiling from the CLI, use the **no debug dpe statistics** command.

After you enable the traffic statistics feature, you can view the traffic statistics from the *perfstat.log* file or analyze the data by using the **runStatAnalyzer.sh** tool.

You can view the traffic statistics by using the administrator user interface. Choose **Servers > DPEs > Manage Device Provisioning Page > View Device Provisioning Engines Details.**