Cisco Broadband Access Center 3.7 DPE CLI Reference

March 30, 2012

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Text Part Number: OL-25685-01

Cisco Broadband Access Center 3.7 DPE CLI Reference

CONTENTS

Preface

The *Cisco Broadband Access Center DPE CLI Reference* describes the command line interface (CLI) commands that support Cisco Broadband Access Center, which is called Cisco BAC throughout the guide.

This chapter provides an outline of the other chapters in this guide, and demonstrates the styles and conventions used in the guide.

This chapter contains:

Audience

This guide is written for those using the CLI of the Cisco BAC Device Provisioning Engine (DPE).

Organization

This guide includes the following sections:

Section	Title	Description
Chapter 1	Introduction to the Cisco Broadband Access Center CLI	Describes the DPE CLI and explains how to access the DPE.
Chapter 2	System Commands	Describes commands used to manage various system aspects of the DPE.
Chapter 3	DPE Configuration Commands	Describes commands used to configure the DPE.
Chapter 4	Auth Service Configuration Commands	Describes commands used to manage and monitor aspects of Device Provisioning Engine (DPE)
Chapter 5	Debug Commands for Auth Service	Describes commands used to debug the CWMP technology.

Section	Title	Description
Chapter 6	CWMP Technology Commands	Describes commands related to the CWMP technology.
Chapter 7	SNMP Agent Commands	Describes commands related to the SNMP agent process on the DPE.
Chapter 8	Log and Debug Commands for DPE	Describes commands related to log management of the DPE.
Chapter 9	Debug Commands for CWMP Technology	Describes commands related to debugging of the CWMP technology.
Chapter 10	Support and Troubleshooting Commands	Describes commands used to support and troubleshoot the DPE.
	Glossary	Defines terminology used in this guide and generally applicable to the technologies being discussed.

Conventions

This document uses the following conventions:

Convention	Indication
bold font	Commands and keywords and user-entered text appear in **bold** font.
italic font	Document titles, new or emphasized terms, and arguments for which you supply values are in *italic* font.
[ ]	Elements in square brackets are optional.
{ x | y | z }	Required alternative keywords are grouped in braces and separated by vertical bars.
[x | y | z]	Optional alternative keywords are grouped in brackets and separated by vertical bars.
string	A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.
`courier` font	Terminal sessions and information the system displays appear in `courier` font.
< >	Nonprinting characters such as passwords are in angle brackets.
[ ]	Default responses to system prompts are in square brackets.
!, #	An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.

Note Means *reader take note*.

Caution Means *reader be careful*. In this situation, you might perform an action that could result in equipment damage or loss of data.

Product Documentation

Note We sometimes update the printed and electronic documentation after original publication. Therefore, you should also review the documentation on Cisco.com for any updates.

Table 1 describes the product documentation that is available.

Table 1 Product Documentation

Document Title	Location
Cisco Broadband Access Center 3.7 Documentation Overview	On Cisco.com at this URL: http://www.cisco.com/en/US/docs/net_mgmt/broadband_access_center/3.7/documentation/overview/Cisco_BAC37_DocOverview.html
Cisco Broadband Access Center 3.7 Release Notes	On Cisco.com at this URL: http://www.cisco.com/en/US/products/sw/netmgtsw/ps529/prod_ release_notes_list.html
Cisco Broadband Access Center 3.7 Installation Guide	On Cisco.com at this URL: http://www.cisco.com/en/US/products/sw/netmgtsw/ps529/prod_ installation_guides_list.html
Cisco Broadband Access Center 3.7 Administrator Guide	On Cisco.com at this URL: http://www.cisco.com/en/US/products/sw/netmgtsw/ps529/prod_maintenance_guides_list.html
Cisco Broadband Access Center 3.7 Integration Developer's Guide	On Cisco.com at this URL: http://www.cisco.com/en/US/products/sw/netmgtsw/ps529/prod_command_reference_list.html
Cisco Broadband Access Center 3.7 Third Party and Open Source Copyrights	On Cisco.com at this URL: http://www.cisco.com/en/US/products/sw/netmgtsw/ps529/products_licensing_information_listing.html

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Subscribe to the *What's New in Cisco Product Documentation* as an RSS feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service. Cisco currently supports RSS Version 2.0.

CHAPTER 1

Introduction to the Cisco Broadband Access Center CLI

This chapter describes how you can start the command line interface (CLI) to access the Cisco Broadband Access Center (Cisco BAC) Device Provisioning Engine (DPE).

Accessing the DPE CLI from a Local Host

To access the DPE CLI, open a Telnet session to port 2323 from a local or remote host.

To access the CLI from a local host, you can enter:

```
# telnet localhost 2323
```

or

```
# telnet 0 2323
```

Accessing the DPE CLI from a Remote Host

To access the CLI from a remote host, enter:

```
# telnet remote-hostname 2323
```

Note If you cannot establish a Telnet connection to the CLI, it is likely that the CLI server is not running. You may need to start the server. To start the server, enter:

```
# /etc/init.d/bprAgent start cli
```

After you access the CLI, you must enter the DPE password to continue. The default login and enable passwords are **changeme**.

For information on how to change the login password and the enable password, see the password, page 2-6, and the enable password, page 2-3, commands, respectively.

Examples

```
bac_host# telnet 0 2323

Trying 0.0.0.0...
Connected to 0.
Escape character is '^]'.

bac_host BAC Device Provisioning Engine


User Access Verification

Password:

bac_host> enable
Password:
bac_host#
```

CHAPTER 2

System Commands

This chapter describes the command line interface (CLI) commands that you can use to manage and monitor aspects of the Cisco Broadband Access Center (Cisco BAC) Device Provisioning Engine (DPE).

Note In Linux, to run system statistics commands like iostat, mpstat and so on, you are required to use the rmp **sysstat-7.0.2-3.el5.x86_64.rmp**.

The system commands that affect the entire DPE are:

aaa authentication

Use this command to configure the CLI to perform local user (login) authentication, or remote TACACS+ user authentication. This setting applies to all Telnet and console CLI interfaces.

TACACS+ is a TCP-based protocol that supports centralized access control for large numbers of network devices and user authentication for the DPE CLI. A DPE supports multiple users (and their individual usernames) and the login and enable passwords configured at the TACACS+ server, using TACACS+.

Syntax Description

aaa authentication *mode*

mode specifies either:

- **local**—In this mode, user authentication is enabled through a local login.
- **tacacs**—In this mode, the CLI sequentially attempts a TACACS+ exchange with each server in the TACACS+ server list. The attempts continue for a specified number of retries.

  If the end of the server list is reached before a successful protocol exchange occurs, the local authentication mode is automatically enabled. In this manner, you can gain access to the CLI even if the TACACS+ service is completely unavailable.

Note TACACS+ authentication prompts you for your TACACS+ configured username and password; local authentication, however, prompts only for the local configured password.

Defaults

The CLI user's login authentication is, by default, enabled in the local mode.

Examples

```
dpe# aaa authentication tacacs
% OK
```

disable

Use this command to exit from the privileged mode on the DPE. When the disabled mode is activated, only the commands that allow viewing the system configuration, are available on the CLI.

Syntax Description

No keywords or arguments.

Examples

```
dpe# disable
dpe>
```

enable

Use this command to enable the privileged mode on the DPE. Viewing system configuration does not require the privileged mode. However, you can change the system configuration, state, and data, only in the privileged mode.

After entering the command, you are prompted to enter the local, configured, enable password. For information on setting the password for the privileged mode, see enable password, page 2-3.

Syntax Description

No keywords or arguments.

Examples

```
dpe> enable
Password:
dpe#
```

enable password

Use this command to change the local password for accessing the DPE in the privileged mode. You can change the enable password only in the privileged mode.

After the password is changed, all users who, from that point onward, attempt to enter into the privileged mode are required to use the new password.

Note This command does not change the login password; it only changes the local enable password.

Syntax Description

When entering the **enable password** command, you can provide the password on the command line or when prompted.

enable password *password*

password—Specifies the local configured password currently in effect or, optionally, provides a new password. If you omit this parameter, you are prompted for the password.

Examples

Note In these examples, please note the different password messages that might appear.

Example 1

```
dpe# enable password
New enable password:
Retype new enable password:
Password changed successfully.
```

This result occurs when you are prompted to enter the password, and the password is changed successfully.

Example 2

```
dpe# enable password
New enable password:
Retype new enable password:
Sorry, passwords do not match.
```

This result occurs when the password is entered incorrectly.

Example 3

```
dpe# enable password cisco
Password changed successfully
```

This result occurs when you enter the password without being prompted, and the password is changed successfully.

exit

Use this command to close a Telnet connection to the DPE and return to the login prompt. After running this command, a message indicates that the Telnet connection has been closed.

Syntax Description

No keywords or arguments.

Examples

```
dpe# exit
% Connection closed.
```

help

Use this command to display a help screen to assist you in using the DPE CLI. If you need help on a particular command, or to list all available commands, enter *command* **?** or **?**, respectively.

After entering the command, a prompt appears, explaining how you can use the help function.

Command Types

Two types of help are available:

- Full help is available when you enter a command argument, such as **show ?**, and describes each possible argument.
- Partial help is provided when you enter an abbreviated argument and want to know what arguments match the input; for example, **show c?**.

Syntax Description

No keywords or arguments.

Examples

Note In these examples, please note the different help messages that might appear.

Example 1

```
dpe# help
Help may be requested at any point in a command by entering a question mark '?'. If
nothing matches, the help list will be empty and you must backup until entering a '?'
shows the available options.

Two styles of help are provided:

1. Full help is available when you are ready to enter a command argument (e.g. "show ?")
and describes each possible argument.

2. Partial help is provided when an abbreviated argument is entered and you want to know
what arguments match the input (e.g. "show c?").
```

This result occurs when you use the **help** command.

Example 2

```
dpe# show ?
  bundles          Shows the archived bundles.
  clock            Shows the current system time.
  commands         Shows the full command hierarchy.
  cpu              Shows the current CPU usage.
  device-config    Show device configuration.
  disk             Shows the current disk usage.
  dpe              Shows the status of the DPE process if started.
  files            Shows files in DPE cache.
  hostname         Shows the system hostname.
  ip               Shows IP configuration details.
  log              Shows recent log entries.
  memory           Shows the current memory usage.
  running-config   Shows the appliance configuration.
  version          Shows DPE version.
```

This result occurs when you invoke the full help function for a command; in this instance, **show ?**.

Example 3

```
dpe# show c?
clock     commands  cpu
dpe# show clock
Sat Jul 15 01:43:19 EDT 2006
```

This result occurs when you invoke the partial help function for arguments of a command; in this instance, **show clock**.

password

Use this command to change the local system password, which you use to access the DPE and is different from the one used to access the privileged mode on the DPE. The system password is changed automatically for future logins, by using the administrator account.

Note The changes that you introduce through this command take effect for new users, but users who are currently logged on are not disconnected.
If TACACS+ user authentication is used, the local system password is used only if the DPE is unable to communicate with a TACACS+ server.

Syntax Description

password *password*

password—Identifies the new DPE password.

Examples

Example 1

```
dpe# password
New password:
Retype new password:
Password changed successfully.
```

This result occurs when you are prompted for the password, and the password is changed successfully.

Example 2

```
dpe# password
New password:
Retype new password:
Sorry, passwords do not match.
```

This result occurs when the password is entered incorrectly.

Example 3

```
dpe# password cisco
Password changed successfully.
```

This result occurs when the password is changed (using an approach easier for scripting).

show

Use the **show** command to view system settings and status. Table 2-1 lists the various keywords that you can use with the **show** command.

Table 2-1 List of show Commands

Command Usage	Syntax Description	Returned Values and Examples
show clock		
Displays the current system time and date	No keywords or arguments.	`dpe# show clock` Mon Jun 16 04:21:25 EDT 2006
show commands		

Displays all commands on the DPE depending on the mode (privileged or disabled) in which you access the CLI.	No keywords or arguments.	**Example 1**
		`dpe> show commands`
		`> enable`
		`> exit`
		`> help`
		`> show bundles`
		`> show clock`
		`> show commands`
		`> show cpu`
		`> show disk`
		`> show dpe`
		`> show dpe config`
		`> show files`
		`> show hostname`
		`> show ip`
		`> show ip route`
		`> show log`
		`> show log last <1..9999>`
		`> show memory`
		`> show running-config`
		`> show version`
		`> uptime`
		This result occurs in the disabled mode.
		Note The output presented in these examples is trimmed.
		Example 2
		`dpe# show commands`
		`> aaa authentication local`
		`> aaa authentication tacacs`
		`> clear bundles`
		`> clear cache`
		`> debug dpe cache`
		`> debug dpe connection`
		`> debug dpe dpe-server`
		`> debug dpe statistics`
		`> debug on`
		`> debug service cwmp 1 client-auth-all`
		`> debug service cwmp 1 client-auth-failures`
		`> debug service cwmp 1 extension`
		`> debug service cwmp 1 firmware`
		`[more]`
		This result occurs in the privileged mode.

Table 2-1 List of show Commands (continued)

Command Usage	Syntax Description	Returned Values and Examples
show cpu		
Identifies CPU usage for the device on which the DPE is running. After the command is entered, CPU activities and statistics appear.	No keywords or arguments.	When you enter **show cpu**, the DPE returns per-processor statistics, as defined for the following headers, in tabular form: **Note** Unless otherwise noted, all values are events per second. • CPU—Processor ID. • minf—Minor faults. • mjf—Major faults. • xcal—Inter-processor cross-calls. • intr—Interrupts. • ithr—Interrupts as threads (not counting clock interrupt). • csw—Context switches. • icsw—Involuntary context switches. • migr—Thread migrations (to another processor). • smtx—Spins on mutexes. • srw—Spins on readers' or writers' lock. • syscl—System calls. • usr—User time (percent). • sys—System time (percent). • wt—Wait time (percent). • idl—Idle time (percent).
show disk		
Identifies the disk that the DPE is currently using. After the command is entered, the disk drive statistics appear.	**No keywords or arguments.**	When you enter **show disk**, the DPE returns values for the following headers: • Filesystem—Indicates path of the file system. • Size—Indicates size of the file system (Kb). • Used—Indicates used disk space (Kb). • Avail—Indicates available disk space (Kb). • Capacity—Indicates capacity of the disk (percent). • Mounted on—Indicates the resources on which the filesystem is mounted. Resources are usually directories.

Table 2-1 List of show Commands (continued)

Command Usage	Syntax Description	Returned Values and Examples
show files		
Identifies the external files cached at the DPE.	No keywords or arguments	dpe# **show files** The list of files currently in DPE cache filename size sample-firmware-image.bin 4239368 DPE caching 1 external files. Listing the first 1 files, 0 files omitted
show hostname		
Displays the DPE hostname	No keywords or arguments.	dpe# **show hostname** hostname = BAC_host
show ip		
Shows the current general IP settings of the DPE. These are the settings used when the DPE is rebooted.	No keywords or arguments.	dpe# **show ip** hostname = BAC_host domainname = abc.com gateway = 10.10.20.10

Table 2-1 List of show Commands (continued)

Command Usage	Syntax Description	Returned Values and Examples
show ip route		
Shows the IP routing table of the DPE, including any custom routes. The default gateway is indicated by the G flag in the flags column.	No keywords or arguments.	When you enter **show ip route**, the DPE returns the routing table with values for the following headers: • Destination—Indicates the destination network or destination host. • Mask—Indicates the subnet mask associated with the route. • Gateway—Indicates the address of the outgoing interface. • Device—Indicates the network interfaces used for the route. • Mxfrg—Indicates the Path Maximum Transfer Unit. • Rtt—Indicates the time (in minutes) remaining before the route expires. • Ref—Indicates the current number of active uses for the route. • Flg—Indicates the state of the route, which could be: – U—Up. – H—To a host rather than to a network. – G—To a gateway. • Out—Identifies the number of packets sent out from this interface or route. • In/Fwd—Identifies the number of packets received through this interface or route.

Table 2-1 List of show Commands (continued)

Command Usage	Syntax Description	Returned Values and Examples
show memory		
Identifies how much current memory and swap space are available on the device running the DPE.	No keywords or arguments.	When you enter **show memory**, the DPE returns values for the following headers: • kthr—Indicates the number of kernel threads in each of the three following states: – r—Run queue. – b—Processes blocked while waiting for I/O. – w—Idle processes that have been swapped. • memory—Indicates usage of virtual and real memory. This could be: – swap—Free, unreserved swap space (Kb). – free—Free memory (Kb). • page—Indicates page faults and paging activity (units per second). – re—Displays pages reclaimed from the free list. – mf—Displays minor faults. – pi—Displays pages in memory (Kb/s). – po—Displays pages out of memory (Kb/s). – fr—Displays activity of the page scanner that has been freed (Kb/s). – de—Displays pages freed after writes (Kb/s). – sr—Displays the number of pages that have been scanned (pages). • disk—Indicates the number of disk operations per second. The S columns represent different disks on the system. • faults—Indicates the trap or interrupt rates (per second). – /in: Interrupts – sy: System calls – cs: Context switches • cpu—Indicates the usage of CPU time. – us—User time (percent) – sy—System time (percent) – id—Idle time (percent)

Table 2-1 List of show Commands (continued)

Command Usage	Syntax Description	Returned Values and Examples
show running-config		

Displays the current configuration of the DPE.	No keywords or arguments.	`dpe# show running-config`
		`dpe port 49186`
		`dpe rdu-server server_x.cisco.com 49187`
		`service cwmp 1 client-auth digest`
		`service cwmp 1 enabled true`
		`service cwmp 1 port 7547`
		`service cwmp 1 ssl cipher all-cipher-suites`
		Note The output presented in this example is trimmed.

show version		
Identifies the current version of DPE software.	No keywords or arguments.	`dpe# show version` `Version: BAC 3.5 (bac_3_5_S_000000000000)`

tacacs-server host

Use this command to add a TACACS+ server to the end of the TACACS+ client's list of TACACS+ servers. When TACACS+ authentication is enabled, the client attempts user login authentication to each server sequentially in the list until a successful authentication exchange is executed, or the list is exhausted. If the list is exhausted, the client automatically falls back into the local authentication mode (using the local system password).

You have to specify an encryption key for each TACACS+ server. This encryption key is matched with the key configured at the specified TACACS+ server.

To remove a TACACS+ server from the list of TACACS+ servers in the CLI, use the **no** form of this command. For more information, see no tacacs-server host, page 2-13.

Syntax Description

tacacs-server host *host* **key** *encryption-key*

- *host*—Specifies either the IP address or the hostname of the TACACS+ server.
- *encryption-key*—Specifies the encryption key used for each TACACS+ server.

Examples

Example 1

This example adds a TACACS+ server, by using its IP address (10.0.1.1) with an encryption key (hg667YHHj).

```
dpe# tacacs-server host 10.0.1.1 key hg667YHHj
% OK
```

Example 2

This example adds a TACACS+ server, by using its hostname (tacacs1.cisco.com) with an encryption key (hg667YHHj).

```
dpe# tacacs-server host tacacs1.cisco.com key hg667YHHj
% OK
```

no tacacs-server host

Use this command to remove a TACACS+ server from the list of TACACS+ servers in the CLI.

Syntax Description

no tacacs-server host *host*

host—Specifies the IP address or the hostname of the TACACS+ server.

Examples

Example 1

This example removes a TACACS+ server by using its IP address.

```
dpe# no tacacs-server host 10.0.1.1
% OK
```

Example 2

This example removes a TACACS+ server by using its hostname.

```
dpe# no tacacs-server host tacacs1.abc.com
% OK
```

tacacs-server retries

Use this command to set the number of times the TACACS+ protocol exchanges are retried before the TACACS+ client considers a specific TACACS+ server unreachable. When this limit is reached, the TACACS+ client moves to the next server in its TACACS+ server list, or falls back into local authentication mode if the TACACS+ list has been exhausted.

Syntax Description

tacacs-server retries *value*

value—Specifies a dimensionless number from 1 to 100.

Note This value applies to all TACACS+ servers.

Defaults

The number of times the TACACS+ protocol exchanges are retried before the TACACS+ client considers a specific TACACS+ server unreachable is, by default, set to 2.

Examples

```
dpe# tacacs-server retries 10
% OK
```

tacacs-server timeout

Use this command to set the maximum time that the TACACS+ client waits for a TACACS+ server response before it considers the protocol exchange to have failed.

Syntax Description

tacacs-server timeout *value*

value—Specifies the duration for which the CLI waits for a TACACS+ server response. This value must be within the range of 1 to 300 seconds.

Note This value applies to all TACACS+ servers.

Defaults

The maximum time that the CLI waits for a TACACS+ server response before it times out is, by default, 5 seconds.

Examples

```
dpe# tacacs-server timeout 10
% OK
```

uptime

Use this command to identify how long the system has been operational. This information is useful when determining how frequently the device is rebooted. It is also helpful when checking the reliability of the DPE when it is in a stable condition.

Syntax Description

No keywords or arguments.

Examples

```
dpe# uptime
11:42pm  up 72 day(s),  8:02,  1 user,  load average: 0.00, 0.02, 0.02
```

CHAPTER 3

DPE Configuration Commands

This chapter describes the command line interface (CLI) commands that you can use to manage and monitor the Cisco Broadband Access Center (Cisco BAC) Device Provisioning Engine (DPE).

The commands described in this chapter are:

clear cache

Use this command to erase the entire DPE cache and reset the server to a clean state. When you restart the DPE, it connects to the RDU and rebuilds the cache from the information stored in the RDU database.

Ensure that you stop the DPE before erasing the DPE cache by running the **dpe stop** command. For more information, see dpe start | stop, page 3-6.

You should clear the cache only when the DPE encounters a major problem. Running this command forces the DPE to rebuild or repopulate its device cache. This process may take a long time to complete.

After the command is entered, the DPE cache is cleared and a prompt appears to indicate how much disk space was cleared as a result. If the cache could not be cleared, the reason for the failure appears.

Syntax Description

No keywords or arguments.

Examples

Example 1

```
dpe# clear cache
Clearing DPE cache...
+ 417792 bytes cleared.
```

This result occurs when the cache is successfully cleared.

Example 2

```
dpe# clear cache
DPE must be stopped before clearing cache.
```

This result occurs when the DPE has not yet been stopped.

Example 3

```
dpe# clear cache
Clearing DPE cache...
+ Cache already cleared.
```

This result occurs when the cache has already been cleared.

dpe port

Use this command to specify the port the DPE uses to communicate with the RDU.

You must stop the DPE before changing its port number. If you run this command on an operational DPE, the following error message appears:

```
ERROR: DPE must be stopped before changing the port number.
```

The changes that you introduce through this command do not take effect until you restart the DPE. For information on stopping and starting the DPE, see dpe start | stop, page 3-6.

Syntax Description

dpe port *port*

port—Identifies the DPE port number that is used for connecting to the RDU.

Defaults

The port that the DPE uses is, by default, 49186.

Examples

```
dpe# dpe port 49186
% OK
```

dpe provisioning-group primary

Use this command to specify the DPE as a member of a specified primary provisioning group. Most DPEs are configured with one primary provisioning group. However, you can assign the DPE to multiple provisioning groups, if required.

If you restart the DPE, while assigning new provisioning groups that have a large number of devices, it can take a long time, depending on the number of devices in your network and the size of the devices' configurations. This delay is because the cache for each provisioning group has to be synchronized; or, for new provisioning groups, completely rebuilt.

Note In normal situations, you must change the provisioning groups only when the DPE is first deployed on the network.

After you use this command, run the **dpe reload** command so that the changes take effect. See dpe reload, page 3-5, for additional information.

To remove configured primary provisioning groups, use the **no** form of this command. For more information, see dpe rdu-server, page 3-5.

Syntax Description

dpe provisioning-group primary *name* [*name**]

- *name*—Identifies the assigned primary provisioning group.
- *name**—Allows the entry of multiple provisioning groups. When specifying multiple provisioning groups, you must insert a space between their names.

Note Depending on the technology deployed, you can specify one or more provisioning groups to which the DPE can belong.

Example 1

```
dpe# dpe provisioning-group primary PrimaryProvGroup
% OK (Requires DPE restart "# dpe reload")
```

Example 2

```
dpe# dpe provisioning-group primary provisioning-grp-1 provisioning-grp-2
% OK (Requires DPE restart "# dpe reload")
```

dpe rdu-server

Use this command to identify the RDU to which this DPE connects. Normally, you configure the RDU on the default port, but for security reasons, you could configure it to run on a nondefault port.

After you use this command, run the **dpe reload** command so that the changes take effect. See dpe reload, page 3-5, for additional information.

Syntax Description

dpe rdu-server *{host | ip} port*

- *host*—Identifies the fully qualified domain name of the host on which the RDU is running.
- *ip*—Identifies the IP address of the RDU.
- *port*—Identifies the port number on which RDU is listening for DPE connections (by default, it is 49187).

Examples

Example 1

```
dpe# dpe rdu-server rdu.cisco.com 49187
% OK (Requires DPE restart "# dpe reload")
```

This result occurs when you specify the fully qualified domain name of the RDU host.

Example 2

```
dpe# dpe rdu-server 10.10.20.1 49187
% OK (Requires DPE restart "# dpe reload")
```

This result occurs when you specify the IP address of the RDU host.

dpe reload

Use this command to restart the DPE, which must be operational before you reload it. If the DPE has not stopped within 60 seconds, the Cisco BAC process watchdog (bprAgent) forces the DPE to stop, and an alert message, indicating that this has occurred, appears. After that message appears, the DPE restarts.

Syntax Description

No keywords or arguments.

Examples

```
dpe# dpe reload
Process dpe has been restarted
```

dpe shared-secret

Use this command to set the shared secret used for communication with the RDU. Communication fails if the shared secrets, set on the two servers, are not the same.

After you use this command, run the **dpe reload** command so that the changes take effect. See dpe reload, page 3-5, for additional information.

Syntax Description

dpe shared-secret *secret*

secret—Identifies the RDU shared secret.

Defaults

The default shared secret used for communication with the RDU is **secret**.

Examples

```
dpe# dpe shared-secret private
% OK (Requires DPE restart "# dpe reload")
```

dpe start | stop

Use this command to start or stop the DPE.

Syntax Description

dpe start | **stop**

- **start**—Starts the DPE. You can use this command only when the DPE is not running. Even if the DPE starts successfully, it does not guarantee that it will run successfully. Check the DPE log to ensure that the DPE has started correctly. Also, check the log periodically to ensure that no additional errors have occurred.
- **stop**—Stops the DPE. You can use this command only when the DPE is running. If the DPE has not stopped within 60 seconds, the DPE process watchdog forces the DPE to stop, and an alert message, indicating that this has occurred, appears.

Examples

Example 1

```
dpe# dpe start
Process dpe has been started
```

Example 2

```
dpe# dpe stop
dpe is stopped
```

interface ethernet provisioning enabled

Use this command to control whether the Ethernet interface(s) is used to handle provisioning requests. This command isolates the interactions of the DPE with the RDU from its interactions with CPE.

Specifically, the fully qualified domain name of the enabled interface is set as the URL for file downloads that a CPE device performs (for information on setting the FQDN, see interface ethernet provisioning fqdn, page 3-7).

After you use this command, run the **reload** command so that the changes take effect. See dpe reload, page 3-5, for additional information.

Syntax Description

interface ethernet {*intf0* | *intf1*} **provisioning enabled** {**true** | **false**}

- *intf0* | *intf1*—Identifies the Ethernet interface.
- **true**—Indicates that provisioning has been enabled.
- **false**—Indicates that provisioning has been disabled.

Defaults

Provisioning operations for the Ethernet interface(s) is, by default, disabled.

Examples

```
dpe# interface ethernet hme0 provisioning enabled true
% OK (Requires DPE restart "# dpe reload")
```

interface ethernet provisioning fqdn

Use this command to set the fully qualified domain name (FQDN) for a specific interface. The provisioning FQDN is the FQDN that is given to a CPE to contact the specific DPE interface. In CWMP, this FQDN is used to construct the auto-configuration server URL when performing a CPE redirect or similar functions, unless a different value was configured on the provisioning group object at the RDU.

Remember to use the same FQDN for all DPEs in a given provisioning group. If DPEs are located behind the load-balancer, use the FQDN of the load balancer as the interface FQDN, and ensure that it is the same for all DPEs that are part of the same load-balancing group.

Before setting the FQDN for an interface, ensure that provisioning is enabled on that interface. To enable provisioning on an interface, see interface ethernet provisioning enabled, page 3-7.

After you use this command, run the **reload** command so that the changes take effect. See dpe reload, page 3-5, for additional information.

Syntax Description

interface ethernet {*intf0* | *intf1*} **provisioning fqdn** *fqdn*

- *intf0* | *intf1*—Identifies the Ethernet interface.
- *fqdn*—Identifies the fully qualified domain name that is set on the specified interface.

Examples

```
dpe# interface ethernet hme0 provisioning fqdn cisco.com
% OK (Requires DPE restart "> dpe reload")
```

interface ip pg-communication

Use this command to configure the DPE to use the interface identified by the IP address to communicate with other provisioning groups.

If you do not run this DPE configuration command, the DPE always binds to the localhost.

Note The IP address that you specify in this command must exist on the machine and must be active. You can configure only one interface at a time.

When you use this command, run the **reload** command so that the changes take effect. See dpe reload, page 3-5, for additional information.

Syntax Description

interface ip *ip_address* **pg-communication**

ip_address—Specifies the IP address of the interface to be used for communication with other provisioning groups.

The DPE CLI displays the available IP addresses if **?** command is used for the ip_address field.

Examples

```
dpe# interface ip 10.1.1.2 pg-communication
% OK (Requires DPE restart "> dpe reload")
```

show device-config

Use this command to display a device configuration that is cached at the DPE.

If you run this command on an unlicensed DPE, a message similar to the following one appears:

```
This DPE is not licensed. Your request cannot be serviced.
Please check with your system administrator for a DPE license.
```

Syntax Description

show device-config *device-ID*

device-ID—Identifies the device.

Examples

For the purpose of this example, assume that the device ID is *00000C-7816406053*.

```
dpe# show device-config 00000C-7816406053
Properties
    /provisioning/configuration/revision=298f54e
    /provisioning/firmwareConfiguration/revision=1b735cef

    HTTP Configuration

       RoutableIPAddressRecord:
          OPERATION_ID: 2798e7:1341333c80e:80000021
          UPDATE_IP: false
          HAS_ROUTABLE_IP: null

       Data Synchronization Instruction:
          IS_PERSISTENT: true
          IS_AUTO_RUN: true
          DATA_SYNC_PARAMS:
             Inform.DeviceId.ManufacturerOUI: null
             *.DeviceInfo.ModelName: null
             Inform.DeviceId.ProductClass: null
             Inform.DeviceId.Manufacturer: null
             *.ManagementServer.ParameterKey: null
             *.DeviceInfo.HardwareVersion: null
             *.DeviceInfo.SoftwareVersion: null
          FIRMWARE_CHANGED_PARAMS:
             *.DeviceInfo.ModelName
          IGNORE_EMPTY_DATA_SYNC_PARAMS:
             *.ManagementServer.ParameterKey

       Firmware Rules Instruction:
          IS_PERSISTENT: true
          FIRMWARE_RULES:
          Version: 1.0
          Prerequisite Maintenance Window:
             Start Time: 04:00:00
             Duration: 20:00
          Prerequisite Expressions:
             Expression:
                Parameter: InternetGatewayDevice.DeviceInfo.Manufacturer
                Inform Parameter: null
                Rpc Argument: null
                Value: Linksys
                Operator: matchIgnoreCase
             Expression:
                Parameter: null
                Inform Parameter: null
                Rpc Argument: RequestDownload.FileType
                Value: 1 Firmware Upgrade Image
                Operator: match
          Firmware Rules:
             Firmware Rule: LinksysWAG54G2Rule
                Expressions:
                   Expression:
                      Parameter: null
                      Inform Parameter: Inform.EventCode
                      Rpc Argument: null
                      Values: [1 BOOT, 3 SCHEDULED]
                      Operator: match
                   Expression:
                      Parameter: InternetGatewayDevice.DeviceInfo.SoftwareVersion
                      Inform Parameter: null
                      Rpc Argument: null
                      Values: [1.02, 2.02]
```

```
                        Operator: matchIgnoreCase
                  Internal File:
                     Firmware File: sample-firmware-image.bin
                     File Delivery Transport: service http 1
                     FileType: 1 Firmware Upgrade Image
               Firmware Rule: LinksysGenericFirmwareRule
                  Expressions:
                     Expression:
                        Parameter: InternetGatewayDevice.DeviceInfo.SoftwareVersion
                        Inform Parameter: null
                        Rpc Argument: null
                        Value: 66
                        Operator: match
                  External File:
                     File Url: http://10.10.10.10:889/sample-firmware-image.bin
                     Username: test
                     Password: changeme
                     File Size: 3449
                     FileType: 1 Firmware Upgrade Image
            FORCE_FIRMWARE_UPGRADE: false

      Configuration Synchronization Instruction:
         OPERATION_ID: 2798e7:1341333c80e:80000022
         IS_PERSISTENT: true
         CONFIG:
            Version: 1.0
            Configuration Objects / Parameters:
                Parameter Name:
InternetGatewayDevice.ManagementServer.PeriodicInformEnable
                Value: true
                Type: boolean
                ValueType: NORMAL
                Parameter Name:
InternetGatewayDevice.ManagementServer.PeriodicInformInterval
                Value: 86400
                Type: unsignedInt
                ValueType: NORMAL
         CONFIG_REV_NUMBER: 43578702 (298f54e)
         FORCE_CONFIG_UPGRADE: false
         LAST_CONFIGURED_REV_NUMBER:
```

Note The label, ToBeSigned is displayed for the parameters that are designated to be signed. To generate the signed configuration, at least one parameter in the configuration template must be flagged to be signed.

show dpe

Use the **show dpe** command to see if the DPE is running. It also displays the state of the process and, if running, its operational statistics. This command does not indicate if the DPE is running successfully and servicing requests. It only indicates if the process is being executed. However, when the DPE is running, you can use statistics that this command displays to determine if the DPE is successfully servicing requests.

If you run this command on an unlicensed DPE, a message similar to this one appears:

```
This DPE is not licensed. Your request cannot be serviced.
Please check with your system administrator for a DPE license.
```

Syntax Description No keywords or arguments.

Examples

Example 1

```
bacdev1-t5120-2-d6# show dpe
BAC Process Watchdog is running.
Process [dpe] is not running.
```

This result occurs when the DPE is not running.

Example 2

```
bacdev1-t5120-2-d6# show dpe
BAC Process Watchdog is running.
Process [dpe] is running.

Broadband Access Center [BAC 3.7 (SOL_BAC3_7_20111206_0220_143)].
Connected to RDU [bacdev1-t5120-2-d6].
Caching [0] device configs and [1] files.
0 sessions succeeded and 0 sessions failed.
0 file requests succeeded and 0 file requests failed.
0 immediate device operations succeeded, and 0 failed.
0 home PG redirections succeeded, and 0 failed.
Using signature key name [] with a validity of [3600].
Abbreviated ParamList is enabled.
Running for [1] days [1] hours [40] mins [14] secs.
```

This result occurs when the DPE is running.

show dpe config

Use this command to display the current settings on the DPE. After you enter the command, the DPE configuration appears.

Syntax Description No keywords or arguments.

Examples

```
dpe# show dpe config
dpe port         = 49186
rdu host         = host.abc.com
rdu port         = 49187
primary groups   = default
secondary groups = [no value]
```

show run

Use this command to display the current configuration settings on the DPE.

Syntax Description No keywords or arguments.

Examples

```
dpe# show run
aaa authentication local
chatty-client filter enabled false
chatty-client quiet-hits-to-leave-throttled-cwmp 5
chatty-client quiet-hits-to-leave-throttled-httpfile 5
chatty-client quite-time-interval 10000
chatty-client sample-hits-to-throttle-cwmp 10
chatty-client sample-hits-to-throttle-httpfile 5
chatty-client sample-time-interval 30000
debug service cwmp 1 errors
debug service cwmp 1 http-details
debug service http framework
dpe port 49186
dpe provisioning-group primary test-other
dpe rdi-server bacdev2-t5220-1-d4 49187
dpe shared-secret <value is set>
interface ip 10.86.147.122 pg-communication
log level 5-notification
no debug
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
```

chatty-client filter enabled

Use this command to enable or disable the Chatty-client filter on the DPE. When you enable this filter, the DPE detects and throttles the devices that make excessive number of TR-069 or HTTP file server calls.

Syntax Description

chatty-client filter enabled {**true** | **false**}

- **true**—Enables the Chatty-client filter.
- **false**—Disables the Chatty-client filter.

Defaults

The chatty-client filter is, by default, enabled.

Examples

```
dpe# chatty-client filter enabled true
% ok
```

chatty-client sample-time-interval

Use this command to specify the duration for which the DPE monitors the activity of a device. If a device generates more than the specified number of events within the sample time interval, the DPE moves the device to a throttled state.

Syntax Description

chatty-client sample-time-interval *time*

time—Identifies the sample time interval.

Defaults

The sample time interval is, by default, 30000 milliseconds.

Examples

```
dpe# chatty-client sample-time-interval 30000
% ok
```

chatty-client quiet-time-interval

Use this command to configure the quiet time interval for the Chatty clients. The DPE monitors the activities of the throttled device for the specified duration. If the device generates less than the specified number of events within the quiet time interval, the DPE moves the device to a quiet state, otherwise it resets the device to a throttled state.

Syntax Description **chatty-client quiet-time-interval** *time*

time—Identifies the quiet time interval.

Defaults The quiet time interval is, by default, 10000 milliseconds

Examples
```
dpe# chatty-client quiet-time-interval 10000
% ok
```

chatty-client sample-hits-to-throttle-cwmp

Use this command to configure the number of CWMP events received from a device during the sample time interval. If the device generates more than the specified number of CWMP events within the sample time interval, the DPE moves the device to a throttled state.

Syntax Description **chatty-client sample-hits-to-throttle-cwmp** *number_of_cwmp_events*

number_of_cwmp_events—Identifies the number of CWMP events received from a device during the sample time interval.

Defaults The number of CWMP events received from a device during the sample time interval is, by default, 20.

Examples
```
dpe# chatty-client sample-hits-to-throttle-cwmp 20
% ok
```

chatty-client sample-hits-to-throttle-httpfile

Use this command to configure the number of HTTP file requests received from a device during the sample time interval. If the device generates more than the specified number of HTTP file requests within the sample time interval, the DPE moves the device to a throttled state.

Syntax Description **chatty-client sample-hits-to-throttle-httpfile** *number_of_HTTP_file_requests*

number_of_HTTP_file_requests—Identifies the number of HTTP file requests received from a device during the sample time interval.

Defaults The number of HTTP file requests received from a device during the sample time interval is, by default, 10.

Examples

```
dpe# chatty-client sample-hit-to-throttle-httpfile 20
% ok
```

chatty-client quiet-hits-to-leave-throttled-cwmp

Use this command to configure the number of CWMP events received from a device during the quiet time interval.

If the device generates more than the specified number of CWMP events within the quiet time interval, the DPE moves the device to a throttled state. If the number of CWMP events received from the device during the quiet time interval is less than the value configured for the quiet-hits-to-leave-throttled property, the DPE restores the device to the normal state.

Syntax Description

chatty-client quiet-hits-to-leave-throttled-cwmp *number_of_cwmp_events*

number_of_cwmp_events—Identifies the number of CWMP events received from a device during the quiet time interval.

Defaults

The number of CWMP events received from a device during the quiet time interval is, by default, 5.

Examples

```
dpe# chatty-client quiet-hits-to-leave-throttled-cwmp 20
% ok
```

chatty-client quiet-hits-to-leave-throttled-httpfile

Use this command to configure the number of HTTP file requests received from a device during the quiet time interval.

If the device generates more than the specified number of HTTP file requests within the quiet time interval, the DPE moves the device to a throttled state. If the number of HTTP file requests received from the device during the quiet time interval is less than the value configured for the quiet-hits-to-leave-throttled property, the DPE restores the device to the normal state.

Syntax Description

chatty-client quiet-hits-to-leave-throttled-httpfile *number_of_HTTP_file_requests*

number_of_HTTP_file_requests—Identifies the number of HTTP file requests received from a device during the quiet time interval.

Defaults

The number of HTTP file requests received during the quiet time interval is, by default, 5.

Examples

```
dpe# chatty-client quiet-hits-to-leave-throttled-httpfile 20
% ok
```

show chatty-client

Use this command to display the list of devices that make an excessive number of TR-069 or HTTP file server calls.

Syntax Description No keywords or arguments.

Examples

```
dpe# show chatty-client
Service     Client ID
CWMP        1-AP-1
CWMP        7-AP-8
CWMP        8-AP-8
```

The chatty client list is sorted by service type and device identifier.

dpe service-auth acl-property

The name of the property that contains the device's white list.

Syntax Description **dpe service-auth acl-property** *property*

property - The property that contains the device's white list.

Defaults: The property that the DPE uses, by default, FC-ACL.

Examples:

```
dpe# dpe service-auth acl-property FC-ACL
% OK (Requires DPE restart "# dpe reload")
```

dpe service-auth authentication enable

Enables or disables Authentication of the HNB in the DPE.

Defaults: By default, authentication is enabled.

- **true** - Enables authentication.
- **false** - Disables authentication.

Examples:

```
dpe# dpe service-auth authentication enable true
% OK (Requires DPE restart "# dpe reload")
```

dpe service-auth authorization enable

Enables or disables Authorization of the HNB in the DPE.

Defaults: By default, authorization is enabled.

- **true** - Enables authorization.
- **false** - Disables authorization.

Examples:

```
dpe# dpe service-auth authorization enable true
% OK (Requires DPE restart "# dpe reload")
```

dpe service-auth xml-schema enable

Enables or disables XML schema validation in Auth service.

Defaults: By default, XML schema validation is disabled.

- **true** - Enables XML schema validation.
- **false** - Disables XML schema validation.

Examples:

```
dpe# dpe service-auth xml-schema enable true
% OK (Requires DPE restart "# dpe reload")
```

dpe service-auth authorization-property

The name of the property to use when performing Authorization.

The property that contains the Femto gateway FQDN.

Syntax Description **dpe service-auth authorization-property** *property*

property - The property that contains the Femto gateway FQDN.

Defaults: The property that the DPE uses, by default, FC-FGW-FQDN.

Examples:

```
dpe# dpe service-auth authorization-property FC-FGW-FQDN
% OK (Requires DPE restart "# dpe reload")
```

dpe service-auth radius-authorization-property

The name of the RADIUS attribute to use when performing authorization. The name of the property that contains the Femto gateway IP.

Syntax Description **dpe service-auth radius-authorization-property** *property*

property - The property that contains the Femto gateway IP.

Defaults: The property that the DPE uses, by default, NAS-IP-Address.

Examples:
```
dpe# dpe service-auth radius-authorization-property NAS-IP-Address
% OK (Requires DPE restart "# dpe reload")
```

dpe car shared-secret

Use this command to set the shared secret used for communication with the CAR EP. Communication fails if the shared secrets, set on the two servers, are not the same.

After you use this command, run the **dpe reload** command so that the changes take effect. See dpe reload, page 3-5, for additional information.

Syntax Description **dpe car shared-secret** *secret*

secret - Identifies the CAR EP shared secret.

Defaults: The default shared secret used for communication with the CAR EP is secret.

Examples:
```
dpe# dpe shared-secret private
% OK (Requires DPE restart "# dpe reload")
```

dpe cnrquery client-port

Use this command to set Lease Query Client Port. The port for lease query to bind to.

After you use this command, run the **dpe reload** command so that the changes take effect. See dpe reload, page 3-5, for additional information.

Syntax Description

dpe cnrquery client-port *port*

port -Identifies the port for lease query to bind to.

Defaults:

The default port for lease query to bind to is 67.

Examples:

```
dpe# dpe cnrquery client-port 23
% OK (Requires DPE restart "# dpe reload")
```

dpe cnrquery client-socket-address

Use this command to set Lease Query interface address.

After you use this command, run the **dpe reload** command so that the changes take effect. See dpe reload, page 3-5, for additional information.

Syntax Description

dpe cnrquery client-socket-address *address*

address - Identifies the address for lease query to bind to.

Defaults:

The default address of this service is 0.0.0.0:67.

Examples:

```
dpe# dpe cnrquery client-socket-address 127.0.0.1:67
% OK (Requires DPE restart "# dpe reload")
```

dpe cnrquery echo

Use this command to indicate whether the DHCP lease query must use CNR echo.

Syntax Description **dpe cnrquery echo** *{true|false}*

By default, CNR echo is disabled.

- **true** - Enables CNR echo.
- **false** - Disables CNR echo.

Defaults: The default value for the flag indicating that the DHCP lease query must use CNR echo is False.

Examples:

```
dpe cnrquery echo true
% OK
```

dpe cnrquery giaddr

Use this command to set the address for GIADDR to use when sending lease queries.

After you use this command, run the **dpe reload** command so that the changes take effect. See dpe reload, page 3-5 for additional information.

Syntax Description **dpe cnrquery giaddr** *address*

address -Identifies the address for GIADDR to use when sending lease queries.

Defaults: The default address for GIADDR to use when sending lease queries is localhost.

Examples:

```
dpe# dpe cnrquery giaddr 127.0.0.1
% OK (Requires DPE restart "# dpe reload")
```

dpe cnrquery require-all-answers

Use this command to indicate whether the first response should be returned or else wait for all DHCP servers to respond.

Syntax Description **dpe cnrquery require-all-answers** *{true|false}*

By default, require-all-answers is disabled.

- **true** - Enables require-all-answers.
- **false** - Disables require-all-answers.

Defaults: The default value for flag indicating the first response should be returned or else, wait for all DHCP servers to respond is False.

Examples:

```
dpe cnrquery require-all-answers true
% OK
```

dpe cnrquery retry

Use this command to set the number of times to attempt a retry with a DHCP server before giving up.

Syntax Description **dpe cnrquery retry** *attempts*

attempts - Identifies the number of times to attempt a retry with a DHCP server before giving up.

Defaults: The default attempts for the number of times to attempt a retry with a DHCP server before giving up is 1.

Examples:

```
dpe# dpe cnrquery retry 2
% OK
```

dpe cnrquery server-port

Use this command to set the port number used to send the DHCP messages.

Syntax Description **dpe cnrquery server-port** *port*

port - Identifies the port number used to send the DHCP messages.

Defaults: The default port number used to send the DHCP messages is 67.

Examples:
```
dpe# dpe cnrquery server-port 67
% OK (Requires DPE restart "# dpe reload")
```

dpe cnrquery threads

Use this command to set the maximum number of threads for lease query reads.

Syntax Description **dpe cnrquery threads** *threads*

threads -Identifies the maximum number of threads for lease query reads.

Defaults: The default maximum number of threads for lease query reads is 16.

Examples:
```
dpe# dpe cnrquery threads 16
% OK (Requires DPE restart "# dpe reload")
```

dpe cnrquery timeout

Use this command to set the amount of milli-seconds that the LeaseQuery will wait for a response from the DHCP server before giving up.

Syntax Description **dpe cnrquery timeout** *timeout*

timeout -Identifies the amount of milli-seconds that the LeaseQuery will wait for a response from the DHCP server before giving up.

Defaults: The default amount of milli-seconds that the LeaseQuery will wait for a response from the DHCP server before giving up is 500.

Examples:

```
dpe# dpe cnrquery timeout 500
% OK
```

CHAPTER 4

Auth Service Configuration Commands

This chapter describes the command line interface (CLI) commands that you can use to configure various settings for the auth service running on the Cisco Broadband Access Center (Cisco BAC) Device Provisioning Engine (DPE).

This is the global syntax of the commands that you can use to configure various settings for the auth service running on the DPE. Using these commands, you can:

- Enable the auth service
- Set the host address for the service
- Set the port number for the service
- Configure the service to use HTTP over SSL/TLS

Command Usage	Syntax Description	Examples
service auth *num* enable {true | false}		
Enables or disables the auth service running on the DPE.	*num*—Identifies the auth service, which is always 1. By default, the auth service is enabled. • **true**—Enables the auth service. • **false**—Disables the auth service.	`dpe# service auth 1 enabled true` `% OK (Requires DPE restart "# dpe reload")`
service auth *num* address *address*		
Sets the host address for the auth service running on the DPE.	*num*—Identifies the auth service, which is always 1. *address*—Identifies the host address for the auth service running on the DPE. By default, the host address for the auth service running on the DPE is 127.0.0.1.	`dpe# service auth 1 host address 127.0.0.1` `% OK (Requires DPE restart "# dpe reload")`
service auth *num* port *port*		

Command Usage	Syntax Description	Examples
Identifies the port on which the auth service communicates with the Cisco Access Registrar Extension Points. By specifying a different port number, this command enables the DPE to prevent potential sharing violations among ports used by other applications.	• *num* - Identifies the auth service, which is always 1. • *port* - Identifies the port number that is to be used by the service. By default, the auth service is configured to listen on Port 7551.	`dpe# service auth 1 port 7551` `% OK (Requires DPE restart "# dpe reload")`
service auth *num* ssl enabled {true | false}		
Enables or disables the use of HTTP over SSL/TLS for the auth service on the DPE. The auth service will not start up if you do not configure the keystore file and the keystore passwords before restarting the DPE. For information on how to configure a keystore file and keystore passwords, see the *Cisco Broadband Access Center Administrator's Guide, Release 3.6*.	• *num* - Identifies the auth service, which is always 1. • **true** - Enables SSL/TLS transport. • **false** - Disables SSL/TLS transport. This is the default configuration for auth service.	`dpe# service auth 1 ssl enabled true` `% OK (Requires DPE restart "# dpe reload")`

CHAPTER 5

Debug Commands for Auth Service

This chapter describes the command line interface (CLI) commands that you can use to debug the CWMP technology on the Cisco Broadband Access Center (Cisco BAC) Device Provisioning Engine (DPE).

Note Before using any debug command, ensure that DPE debugging is enabled. Run the **debug on** command to enable this function. See debug on, page 8-5 for more information.

The different commands explained in this chapter are:

Debug service auth

This section describes the commands that you use to debug the auth service that runs on the DPE.

Command Usage	Example
debug service auth *num* client-auth-all **no debug service auth *num* client-auth-all**	
Enables debugging of successful and failed client authentication for the auth service. To disable debugging of successful and failed client authentication for the auth service, use the **no** form of this command.	`dpe# debug service auth 1 client-auth-all` `% OK`

Command Usage	Example
debug service auth *num* client-auth-failures **no debug service auth *num* client-auth-failures**	
Enables debugging of the client authentication failures for the auth service. To disable debugging of the client authentication failures of the auth service, use the **no** form of this command.	dpe# **debug service auth 1 client-auth-failures** % OK
debug service auth *num* details **no debug service auth *num* details**	
Enables debugging the low-level details of the auth service running on the DPE. To disable debugging the low-level details of the auth service, use the **no** form of this command.	dpe# **debug service auth 1 details** % OK
debug service auth *num* errors **no debug service auth *num* errors**	
Enables debugging of the request errors for the auth service running on the DPE. To disable debugging of the request errors for the auth service, use the **no** form of this command.	dpe# **debug service auth 1 errors** % OK
debug service auth *num* faults **no debug service auth *num* faults**	
Enables debugging of the error responses of the auth service running on the DPE. To disable debugging of the error responses of the auth service, use the **no** form of this command.	dpe# **debug service auth 1 faults** % OK
debug service auth *num* headers **no debug service auth *num* headers**	
Enables debugging of the request and response headers for the auth service running on the DPE. To disable debugging of the request and response headers for the auth service, use the **no** form of this command.	dpe# **debug service auth 1 headers** % OK

CHAPTER 6

CWMP Technology Commands

This chapter contains information about the command line interface (CLI) commands that you can use to manage and monitor the CPE WAN Management Protocol (CWMP) technology on the Cisco Broadband Access Center (Cisco BAC) Device Provisioning Engine (DPE).

Using the commands described in this chapter, you can configure settings for the CWMP services and the HTTP file services on the DPE. Both services feature individual instances: service 1 and service 2, each of which you must configure separately.

Cisco BAC supports different instances so that you can configure different options for each service. For example, CWMP service 1 is, by default, configured to require HTTP digest authentication; but without supporting HTTP over SSL/TLS.

This service is configured to run on port 7547 and is enabled by default. CWMP service 2 is configured on port 7547 with HTTP over SSL/TLS; but is disabled by default. You can reconfigure any of these defaults for each service to suit your requirements. See Table 6-1 for the default configuration for each service.

Table 6-1 Default Settings for CWMP Technology

	CWMP Service		HTTP File Service	
	Service 1	**Service 2**	**Service 1**	**Service 2**
Mode	Enabled	Disabled	Enabled	Disabled
Authentication	Digest	Digest	Digest	Digest
Port Number	7547	7548	7549	7550
HTTP over SSL/TLS	Disabled	Enabled	Disabled	Enabled

Note You cannot globally enable or disable CWMP-related services. You can enable or disable CWMP features only individually.

The commands described in this chapter are:

- service cwmp, page 6-2
  - service cwmp num allow-unknown-cpe, page 6-3
  - service cwmp num client-auth mode, page 6-4
  - service cwmp num enable {true | false}, page 6-4
  - service cwmp num port port, page 6-4

service cwmp

This is the global syntax of the commands that you can use to configure various settings for the CWMP service running on the DPE. Using these commands, you can:

- Enable the CWMP service
- Specify the instance of the service,
- Configure client authentication and client certificate authentication
- Set the port number for the service
- Configure the service to use HTTP over SSL/TLS.

Use **service cwmp** in conjunction with the commands listed in Table 6-2.

Note When using these commands, you must restart the DPE—unless specified otherwise—for the changes to take effect. To restart the DPE, run the **dpe reload** command (see dpe reload, page 3-5).

Table 6-2 List of service cwmp Commands

Command Usage	Syntax Description	Examples
service cwmp *num* allow-unknown-cpe **no service cwmp *num* allow-unknown-cpe**		
Enables or disables the DPE to request configuration from the RDU for devices unknown to the DPE. Enabling this feature may allow a Denial of Service attack on the RDU. You need not restart the DPE for this command to take effect.	*num*—Identifies the CWMP service, which could be 1 or 2.	`dpe# service cwmp 1 allow-unknown-cpe` `% OK`

Table 6-2 List of service cwmp Commands (continued)

Command Usage	Syntax Description	Examples
service cwmp *num* client-auth *mode*		
Enables or disables client authentication for the CWMP service on the DPE. For a list of authentication options in Cisco BAC, refer to the *Cisco Broadband Access Center Administrator's Guide, Release 3.5, 3.5.1, 3.5.2*.	• *num*—Identifies the CWMP service, which could be 1 or 2. • *mode*—Identifies the client authentication mode for the CWMP service. The client authentication mode could be: – **basic**—Enables Basic HTTP authentication. – **digest**—Enables Digest HTTP authentication. This is the default configuration. – **none**—Disables Basic and Digest authentication. In this mode, the CWMP service uses the Device ID in the Inform message to authenticate CPE. To limit security risks during client authentication, we recommend using the Digest mode (the default configuration). It is not advisable to allow client authentication in the Basic mode, or altogether disable Basic and Digest authentication.	dpe# **service cwmp 1 client-auth digest** % OK (Digest authentication was enabled. Basic authentication was disabled. Requires DPE restart "# dpe reload")
service cwmp *num* enable {true | false}		
Enables or disables the CWMP service running on the DPE.	• *num*—Identifies the CWMP service, which could be 1 or 2. By default, the CWMP service is: – Enabled on service 1. – Disabled on service 2. • **true**—Enables the CWMP service. • **false**—Disables the CWMP service.	dpe# **service cwmp 2 enable true** % OK (Requires DPE restart "# dpe reload")
service cwmp *num* port *port*		
Identifies the port on which the CWMP service communicates with the CPE. By specifying a different port number, this command enables the DPE to prevent potential sharing violations among ports used by other applications.	• *num*—Identifies the CWMP service, which could be 1 or 2. • *port*—Identifies the port number that is to be used by the service. By default, the CWMP service is configured to listen on: – Port 7547 for service 1. – Port 7548 for service 2.	dpe# **service cwmp 1 port 7547** % OK (Requires DPE restart "# dpe reload")

Table 6-2 List of service cwmp Commands (continued)

Command Usage	Syntax Description	Examples
service cwmp session timeout *value*		
Sets the duration for timing out a CWMP session. You need not restart the DPE for this command to take effect.	*value*—Identifies the timeout period for the CWMP session, in milliseconds (ms). The timeout period could be anything between 1000 ms (1 second) and 3000000 ms (50 minutes). By default, the duration for a timeout is set as 60000 ms (60 seconds).	`dpe# service cwmp session timeout 60000` `% OK`
service cwmp *num* external-url *url*		
Configures the DPE to represent externally the specified URL as the URL of the CWMP service.	• *num*—Identifies the CWMP service, which could be 1 or 2. • *url*—Identifies the URL that is to be used for the CWMP service.	`dpe# service cwmp 1 external-url https://192.0.2.1:7547/acs` `% OK`

Table 6-2 List of service cwmp Commands (continued)

Command Usage	Syntax Description	Examples
service cwmp *num* ssl client-auth *mode*		

Enables or disables client certificate authentication using HTTP over SSL/TLS for the CWMP service running on the DPE.
 	
For a list of authentication options in Cisco BAC, refer to the *Cisco Broadband Access Center Administrator's Guide, Release 3.5, 3.5.1, 3.5.2*.
	• *num*—Identifies the CWMP service, which could be 1 or 2.
	
	By default, client certificate authentication with SSL/TLS is:
	– Disabled for service 1.
	– Disabled for service 2.
	• *mode*—Identifies the mode of client certificate authentication for the CWMP service. Cisco BAC supports:
	– **client-cert-generic**—Enables client certificate authentication through SSL/TLS by using a generic certificate common to all CPE or a large subset of CPE.
	
	The client certificate is validated by using the signing certificate authority's public key. This key is preconfigured in the DPE keystore.
	
	This certificate-validation process ensures that the certificate is valid, but does not establish the identity of a device. Therefore, the device identifier is not formed by using the data in the CN field of the client certificate.
	
	Instead, the device identifier is formed by using the data provided using Basic or Digest authentication, or by using the data in the CWMP Inform message.
	– **client-cert-unique**—Enables client certificate authentication through SSL/TLS by using the unique certificate that each CPE provides.
	
	After the client certificate is validated by using the signing certificate authority's public key, the device's unique identifier is formed by using the CN field of the client certificate.
	– **none**—Disables client certificate authentication by using HTTP over SSL/TLS for the CWMP service.
		Example 1
		`dpe# service cwmp 1 ssl client-auth client-cert-generic`
		`% OK (Requires DPE restart "# dpe reload")`
		
		Example 2
		`dpe# service cwmp 1 ssl client-auth client-cert-unique`
		`% OK (Requires DPE restart "# dpe reload")`

Table 6-2 List of service cwmp Commands (continued)

Command Usage	Syntax Description	Examples
service cwmp *num* ssl client-auth client-cert-ext		
Enables the authentication of CPE whose connection that used HTTP over SSL/TLS was terminated at a Load Balancer (Cisco ACE 4710). The ACE extracts information about the SSL session, specifically client certificate fields, from the CPE and inserts that data into various HTTP headers. Cisco BAC then retrieves the CN field from the header ClientCert-Subject-CN to form the unique device identifier. Before enabling this command, ensure that you configure ACE to insert the client certificate fields into the HTTP header. For a list of authentication options in Cisco BAC, refer to the *Cisco Broadband Access Center Administrator's Guide, Release 3.5, 3.5.1, 3.5.2*.	*num*—Identifies the CWMP service, which could be 1 or 2. By default, client certificate authentication by using HTTP over SSL/TLS for the CWMP service is: • Disabled for service 1. • Disabled for service 2.	`dpe# service cwmp ssl 1 client-auth client-cert-ext` `% OK (Requires DPE restart "# dpe reload")`

Table 6-2 List of service cwmp Commands (continued)

Command Usage	Syntax Description	Examples
service cwmp *num* ssl cipher {all-cipher-suites | *value*} **no service cwmp *num* ssl cipher {all-cipher-suites | *value*}**		

Enables or disables authentication between the DPE server and CPE by using cryptographic algorithms, or ciphers, supported by HTTP over SSL/TLS for certificate management and session management.
 	
During an SSL handshake, the DPE server and a CPE identify the strongest cipher suite enabled on both, and use that suite for the SSL session.
 	
Cisco BAC supports a list of cipher suites that you can configure from the DPE command line interface.
 	
For a list of cipher suites supported in Cisco BAC, see Table 6-6.
	• *num*—Identifies the CWMP service, which could be 1 or 2.
	
	• **all-cipher-suites**—Enables all the cipher suites to authenticate a session by using HTTP over SSL/TLS for the CWMP service. This is the default configuration.
	
	The **service cwmp ssl cipher all-cipher-suites** command works only if you have not configured any individual ciphers.
	
	To disable an individual cipher suite, use the **no service cwmp ssl cipher** *value* command.
	
	To disable all ciphers, use the **no service cwmp ssl cipher all-cipher-suites** command.
	
	• *value*—Identifies the individual cipher to be enabled for authenticating a session by using HTTP over SSL/TLS for the CWMP service. You can enable or disable any cipher suite.
	
	Each cipher suite specifies a set of algorithms that are associated with a specific cryptography function.
	
	For a list of cryptography algorithms supported in Cisco BAC, see Table 6-5.
		Example 1
		
		`dpe# service cwmp 1 ssl cipher all-cipher-suites`
		`% OK (Requires DPE restart "# dpe reload")`
		
		Example 2
		
		`dpe# service cwmp 1 ssl cipher ssl_dh_anon_with_des_cbc_sha`
		`% OK (Requires DPE restart "# dpe reload")`

Table 6-2 List of service cwmp Commands (continued)

Command Usage	Syntax Description	Examples
service cwmp *num* ssl enable {true | false}		
Enables or disables use of HTTP over SSL/TLS for the CWMP service on the DPE. The CWMP service will fail to start up if you do not configure the keystore file and the keystore passwords before restarting the DPE. For information on how to configure a keystore file and keystore passwords, see the *Cisco Broadband Access Center Administrator's Guide, Release 3.5, 3.5.1, 3.5.2*.	• *num*—Identifies the CWMP service, which could be 1 or 2. • **true**—Enables SSL/TLS transport. This is the default configuration for service 2. • **false**—Disables SSL/TLS transport. This is the default configuration for service 1.	`dpe# service cwmp 1 ssl enable true` `% OK (Requires DPE restart "# dpe reload")`

Table 6-2 List of service cwmp Commands (continued)

Command Usage	Syntax Description	Examples
service cwmp *num* ssl keystore *keystore-filename keystore-password key-password*		
Sets a keystore file, which contains the provisioning server certificate. This certificate is used to authenticate the provisioning server to the devices by using HTTP over SSL/TLS. This setting is relevant only if the service instance is enabled (as in the case of **service cwmp 2**, which is by default disabled), and the SSL/TLS protocol is enabled for that service. To enable SSL/TLS transport, use the **service cwmp *num* ssl enable true** command.	• *num*—Identifies the CWMP service, which could be 1 or 2. • *keystore-filename*—Identifies the keystore file that you created previously. • *keystore-password*—Identifies the keystore password that you used when you created your keystore file. The keystore password must be between 6 and 30 characters. • *key-password*—Identifies the private key password that you used when you created your keystore file. The private key password must be between 6 and 30 characters.	`dpe# service cwmp 1 ssl keystore example.keystore changeme changeme` `% OK (Requires DPE restart "# dpe reload")`
The DPE ships with a default sample keystore, which contains a self-signed certificate. However, because a CWMP device does not trust a self-signed certificate, you cannot use this keystore to enable HTTP over SSL/TLS to provision a device; instead, you must obtain a signed service provider certificate and keystore. For detailed information, see the *Cisco Broadband Access Center Administrator's Guide, Release 3.5, 3.5.1, 3.5.2*.		

service cwmp-redirect

This is the global syntax of the commands that you can use to configure various settings for the cwmp-redirect service running on the DPE. Using these commands, you can:

- Enable the cwmp-redirect service.
- Configure the number of attempts and retry timeout for querying other provisioning groups.
- Configure the maximum number of devices that the DPE queries for every second.
- Set the status period for sending status request queries.
- View the statistics of cwmp-redirect service running on the DPE.

Use **service cwmp-redirect** in conjunction with the commands listed in Table 6-3.

Table 6-3 List of service cwmp-redirect commands

Command Usage	Syntax Description	Examples
service cwmp-redirect 1 lookup enabled {true | false}		
Enables or disables the DPE to send home provisioning group queries to other provisioning groups when a device is unknown. If a provisioning group responds that the device belongs to its group, the device is redirected to that provisioning group. You must specify an interface for provisioning group communication before you run this command. See interface ip pg-communication, page 3-8. You need not restart the DPE for this command to take effect.	• **true**—Enables the DPE to send home provisioning group queries to other provisioning groups when a device is unknown. • **false**—Prevents the DPE from sending home provisioning group queries to other provisioning groups when a device is unknown.	`dpe# service cwmp-redirect 1 lookup enabled true` `% OK`
service cwmp-redirect 1 respond enabled {true | false}		
Enables or disables the DPE to respond to the home provisioning group queries sent from other provisioning groups. You must specify an interface for provisioning group communication before you run this command. See interface ip pg-communication, page 3-8. You need not restart the DPE for this command to take effect.	• **true**—Enables the DPE to respond to the home provisioning group queries sent from other provisioning groups • **false**—Prevents the DPE from responding to the home provisioning group queries sent from other provisioning groups.	`dpe# service cwmp-redirect 1 lookup respond enabled true` `% OK`

Table 6-3 List of service cwmp-redirect commands (continued)

Command Usage	Syntax Description	Examples
service cwmp-redirect 1 timeout *value*		
Sets the duration for which the DPE waits for a response from the other provisioning groups, after sending a home provisioning group query. You need not restart the DPE for this command to take effect.	*value*—Specifies the duration for which the DPE waits for a response from the other provisioning groups. It must be equal to or greater than 50 milliseconds.	dpe# **service cwmp-redirect 1 timeout 100** % OK
service cwmp-redirect 1 attempts *value*		
Sets the maximum number of attempts made by the DPE to send the home provisioning group queries to the other provisioning groups. You need not restart the DPE for this command to take effect.	*value*—Specifies the maximum number of attempts made by the DPE to send the home provisioning group queries to other provisioning groups. It must be equal to or greater than 1.	dpe# **service cwmp-redirect 1 attempts 3** % OK
service cwmp-redirect 1 limit *value*		
Sets the maximum number of devices that the DPE queries for every second to locate the home provisioning group of the device. You need not restart the DPE for this command to take effect.	*value*—Specifies the maximum number of devices that the DPE queries for every second. It must be equal to or greater than 1.	dpe# **service cwmp-redirect 1 limit 50** % OK
service cwmp-redirect 1 status-period *value*		
Specifies the duration at which the DPE sends status request queries to the DPEs in other provisioning groups. You need not restart the DPE for this command to take effect.	*value*—Specifies the duration at which the DPE sends status request queries to other provisioning groups. It must be equal to or greater than 50 milliseconds.	dpe# **service cwmp-redirect 1 status-period 2500** % OK
service cwmp-redirect 1 retry-after-timeout *value*		
Specifies the timeout after which the DPE informs the device to retry later, if the DPE is not able to establish communication with other DPEs. This can happen because of some error or the home provisioning group of the device cannot be found. You need not restart the DPE for this command to take effect.	*value*—Specifies the timeout after which the DPE informs the device to retry later, if the home provisioning group of the device cannot be found. It must be equal to or greater than 1000 milliseconds.	dpe# **service cwmp-redirect 1 retry-after-timeout 2500** % OK

show service cwmp-redirect 1 statistics

Displays the statistics of the home provisioning group redirection service running on the DPE.

Syntax Description No keywords or arguments

Examples

```
dpe# show service cwmp-redirect 1 statistics
PG            DPE              State      Status RQ/RP    Lookup RQ/RP
Los Angeles   10.86.147.122    Sync       2/1             0/0
Boston        192.168.0.27     Down       15903/0         0/0
New York      192.168.0.2      Down       15903/0         0/0
Chicago       192.168.0.12     Down       15903/0         0/0
```

The output presented in this example is trimmed.

keystore import-pkcs12

Use this command to import existing private key and certificates into a DPE-compatible file used in authenticating the DPE to SSL clients. The **keystore import-pkcs12** command opens a PKCS#12 file, reads the contents, and writes a new keystore in the Sun-proprietary Java keystore format called JKS.

The PKCS#12 file format is a standard used for storing certificates and private keys; for example, an imported certificate from a Microsoft Windows 2000 IIS 5.0 server.

If your private key and certificate are stored in separate files, combine them into a single PKCS#12 file before running the **keystore import-pkcs12** command.

You can use the syntax described in the following example, where the **openssl** command combines the keys in `example.key` and the certificate in the `example.crt file` into the `example.pkcs12` file:
`#` **openssl pkcs12 -inkey example.key -in example.crt -export -out example.pkcs12**

Syntax Description **keystore import-pkcs12** *keystore-filename pkcs12-filename keystore-password* key-password *export-password export-key-password*

- *keystore-filename*—Identifies the JKS keystore file that will be created. If it already exists, it will be overwritten.

  Note Remember to specify the full path of the keystore file.

- *pkcs12-filename*—Identifies the PKCS#12 file from which you intend to import the key and certificate.
- *keystore-password*—Identifies the private key password and the keystore password that you used when you created your keystore file. This password must be between 6 and 30 characters.
- *key-password*—Identifies the password used to access keys within DPE keystore. This password must be between 6 and 30 characters.

- *export-password*—Identifies the password used to decrypt the key in the PKCS#12 file. The export password must be between 6 and 30 characters.
- *export-key-password*—Identifies the password used to access keys within the PKCS#12 keystore. This password must be between 6 and 30 characters.

Examples

```
dpe# keystore import-pkcs12 example.keystore example.pkcs12 changeme changeme changeme
changeme
% Reading alias [1]

 % Reading alias [1]: key with format [PKCS8] algorithm [RSA]

 % Reading alias [1]: cert type [X.509]

 % Created JKS keystore: example.keystore

 % OK
```

service http

This is the global syntax of the commands that you use to configure various settings for the HTTP service running on the DPE. Using these commands, you can:

- Enable the service
- Specify the instance of the service
- Configure client authentication and client certificate authentication
- Set the port number for the service
- Configure the service to use HTTP over SSL/TLS

Use **service http** in conjunction with the list of commands described in Table 6-4.

Note When using these commands, you must restart the DPE—unless specified otherwise—for the changes to take effect. To restart the DPE, run the **dpe reload** command (see dpe reload, page 3-5).

Table 6-4 List of service http Commands

Command Usage	Syntax Description	Examples
service http *num* client-auth *mode*		
Enables or disables client authentication for the HTTP file service on the DPE. For a list of authentication options in Cisco BAC, see the *Cisco Broadband Access Center Administrator's Guide, Release 3.5, 3.5.1, 3.5.2*	• *num*—Identifies the HTTP file service, which could be 1 or 2. • *mode*—Identifies the client authentication mode for the HTTP file service. The client authentication mode could be: – **basic**—Enables Basic HTTP file service authentication. – **digest**—Enables Digest HTTP file service authentication. This is the default configuration. – **none**—Disables Basic and Digest authentication. In this mode, the HTTP file service uses the Device ID in the Inform message to authenticate CPE. To limit security risks during client authentication, Cisco recommends using the Digest mode (the default configuration). It is not advisable to allow client authentication in the Basic mode, or disable Basic and Digest authentication.	`dpe# service http 1 client-auth digest` `% OK (Digest authentication was enabled. Basic authentication was disabled. Requires DPE restart "# dpe reload")`

Table 6-4 List of service http Commands (continued)

Command Usage	Syntax Description	Examples
service http *num* enable {true | false}		
Enables or disables the HTTP file service running on the DPE	• *num*—Identifies the HTTP file service, which could be 1 or 2. By default the HTTP file service is: – Enabled on service 1. – Disabled on service 2. • **true**—Enables the HTTP file service. • **false**—Disables the HTTP file service.	dpe# **service http 2 enable true** % OK (Requires DPE restart "# dpe reload")
service http *num* port *port*		
Identifies the port on which the HTTP file service communicates with a CPE device. If you specify a different port number, this command enables the DPE to prevent potential sharing violations among ports used by other applications.	• *num*—Identifies the HTTP file service, which could be 1 or 2. By default, the HTTP file service is configured to listen on: – Port 7549 for service 1. – Port 7550 for service 2. • *port*—Identifies the port number that is to be used by the service. The **service http port** command does not check if the port number specified is being used by other applications or system utilities.	dpe# **service http 1 port 7549** % OK (Requires DPE restart "# dpe reload")
service http *num* external-url *url*		
Configures the DPE to represent externally the specified URL as the URL of the HTTP file service.	• *num*—Identifies the HTTP file service, which could be 1 or 2. • *url*—Identifies the URL that is to be used for the HTTP file service.	dpe# **service http 1 external-url https://192.0.2.27:7547/acs** % OK

Table 6-4 List of service http Commands (continued)

Command Usage	Syntax Description	Examples
service http *num* ssl client-auth *mode*		

Enables or disables client certificate authentication by using HTTP over SSL/TLS for the HTTP file service running on the DPE.
 	
For a list of authentication options in Cisco BAC, refer to the *Cisco Broadband Access Center Administrator's Guide, Release 3.5, 3.5.1, 3.5.2*.
	• *num*—Identifies the HTTP file service, which could be 1 or 2.
	
	By default, client certificate authentication by using HTTP over SSL/TLS for the HTTP file service is:
	– Disabled for service 1.
	– Disabled for service 2.
	• *mode*—Identifies the mode of client certificate authentication for the HTTP file service. Cisco BAC supports:
	– **client-cert-generic**—Enables client certificate authentication through SSL/TLS by using a generic certificate common to all CPE or a large subset of CPE.
	
	The public key of the signing certificate authority is used to validate the client certificate. This key is preconfigured in the DPE keystore.
	
	This certificate validation process ensures that the certificate is valid, but does not establish identity of a given device.
	
	Therefore, the device identifier is not formed by using the data in the CN field of the client certificate.
	
	Instead, the device identifier is formed by using the data provided using Basic or Digest authentication, or by using the data in the CWMP Inform message.
	– **client-cert-unique**—Enables client certificate authentication through SSL/TLS using the unique certificate provided by each CPE.
	
	After the client certificate is validated by using the signing certificate authority's public key, the device's unique identifier is formed by using the CN field of the client certificate.
	– **none**—Disables client certificate authentication by using HTTP over SSL/TLS.
		Example 1
		`dpe# service http 1 ssl client-auth client-cert-generic`
		`% OK (Requires DPE restart "# dpe reload")`
		
		Example 2
		`dpe# service http 1 ssl client-auth client-cert-unique`
		`% OK (Requires DPE restart "# dpe reload")`

Table 6-4 List of service http Commands (continued)

Command Usage	Syntax Description	Examples
service http *num* ssl client-auth client-cert-ext		
Enables the authentication of CPE whose connection that uses HTTP over SSL/TLS was terminated at a Load Balancer (Cisco ACE 4710). The ACE extracts information about the SSL session, specifically client certificate fields, from the CPE, and inserts that data into various HTTP headers. Cisco BAC then retrieves the CN field from the header ClientCert-Subject-CN to form the unique device identifier. Before you enable this command, ensure that you configure ACE to insert the client certificate fields into the HTTP header. For a list of authentication options in Cisco BAC, refer to the *Cisco Broadband Access Center Administrator's Guide, Release 3.5, 3.5.1, 3.5.2*.	*num*—Identifies the HTTP file service, which could be 1 or 2. By default, client certificate authentication that use HTTP over SSL/TLS for the HTTP file service is: • Disabled for service 1. • Disabled for service 2.	`dpe# service http ssl 1 client-auth client-cert-ext` `% OK (Requires DPE restart "# dpe reload")`

Table 6-4 List of service http Commands (continued)

Command Usage	Syntax Description	Examples
service http *num* ssl cipher {all-cipher-suites | *value*} **no service http *num* ssl cipher {all-cipher-suites | *value*}**		

Enables or disables authentication between the DPE server and CPE by using cryptographic algorithms, or ciphers, that HTTP supports over SSL/TLS for certificate management and session management.
 	
During an SSL handshake, the DPE server and a CPE device identify the strongest cipher suite enabled on both, and use that suite for the SSL session.
 	
Cisco BAC supports a list of cipher suites that you can configure from the DPE command line interface.
 	
For a list of cipher suites that Cisco BAC supports, see Table 6-6.
	• *num*—Identifies the HTTP file service, which could be 1 or 2.
	
	• **all-cipher-suites**—Enables all the cipher suites to authenticate a session by using HTTP over SSL/TLS for the HTTP file service. This is the default configuration.
	
	The **service http ssl cipher all-cipher-suites** command works only if you have not configured any individual ciphers.
	
	To remove an individual cipher suite, use the **no service http ssl cipher** *value* command.
	
	To disable all ciphers, use the **no service http ssl cipher all-cipher-suites** command.
	
	• *value*—Identifies the individual cipher to be enabled for authenticating a session using HTTP over SSL/TLS for the HTTP file service. You can enable or disable any cipher suite.
	
	Each cipher suite specifies a set of algorithms that are associated with a specific cryptography function.
	
	For a list of cryptography algorithms that Cisco BAC supports, see Table 6-5.
		Example 1
		`dpe# service http 1 ssl cipher all-cipher-suites`
		`% OK (Requires DPE restart "# dpe reload")`
		
		Example 2
		`dpe# service http 1 ssl cipher ssl_dh_anon_with_des_cbc_sha`
		`% OK (Requires DPE restart "# dpe reload")`

Table 6-4 List of service http Commands (continued)

Command Usage	Syntax Description	Examples
service http *num* ssl enable {true | false}		
Enables or disables use of HTTP over SSL/TLS for the HTTP file service on the DPE. The HTTP file service will fail to start up if you do not configure the keystore file and the keystore passwords before restarting the DPE. For information on how to configure a keystore file and keystore passwords, refer to the *Cisco Broadband Access Center Administrator's Guide, Release 3.5, 3.5.1, 3.5.2.*	• *num*—Identifies the HTTP file service, which could be 1 or 2. • **true**—Enables SSL/TLS transport. This is the default configuration for service 2. • **false**—Disables SSL/TLS transport. This is the default configuration for service 1.	`dpe# service http 1 ssl enable true` `% OK (Requires DPE restart "# dpe reload")`

Table 6-4 List of service http Commands (continued)

Command Usage	Syntax Description	Examples
service http *num* ssl keystore *keystore-filename keystore-password key-pasword*		
Sets a keystore file, which contains the provisioning server certificate. This certificate is used to authenticate the provisioning server to the devices by using HTTP over SSL/TLS. This setting is only relevant if the service instance is enabled (as in the case of service http 2, which is by default disabled) and HTTP over SSL/TLS is enabled for the service. To enable SSL/TLS transport, use the **service http num ssl enable true** command.	• *num*—Identifies the HTTP file service, which could be 1 or 2. • *keystore-filename*—Identifies the keystore file that you created previously. • *keystore-password*—Identifies the keystore password that you used when you created your keystore file. The keystore password must be between 6 and 30 characters. • *key-password*—Identifies the private key password that you used when you created your keystore file. The private key password must be between 6 and 30 characters.	`dpe# service http 1 ssl keystore example.keystore changeme changeme` `% OK (Requires DPE restart "# dpe reload")`
The DPE ships with a default sample keystore, which contains a self-signed certificate. However, because a CWMP device does not trust a self-signed certificate, you cannot use this keystore to enable HTTP over SSL/TLS to provision a device; instead, you must obtain a signed service provider certificate and keystore. For detailed information on how to obtain a signed service provider certificate and keystore, see the *Cisco Broadband Access Center Administrator's Guide, Release 3.5, 3.5.1, 3.5.2*.		

Selecting Cipher Suites

A typical SSL session requires encryption ciphers to establish and maintain the secure connection. Cipher suites provide the cryptographic algorithms that the SSL/TLS protocol requires to authenticate client/server exchanges, and establish and maintain secure connections.

Table 6-5 defines the cryptography algorithms supported in this release of Cisco BAC:

Table 6-5 Cryptography Algorithms Supported in Cisco BAC

Cryptography Function	Algorithms Supported in Cisco BAC
SSL versions	SSL version 3.0 and Transport Layer Security (TLS) version 1.0
Public key exchange and key agreement algorithms	• RSA (key exchange and key agreement algorithm) The Rivest, Shamir, and Adelman algorithm used for encryption and digital signatures. - 512-bit, 768-bit, 1024-bit, and 2048-bit • DSA (certificate signing algorithm) The Digital Signature Algorithm used as part of the Digital Signature Standard (DSS). - 512-bit, 768-bit, and 1024-bit • Diffie-Hellman (key exchange algorithm) - 512-bit, 768-bit, 1024-bit, and 2048-bit

Table 6-5 Cryptography Algorithms Supported in Cisco BAC

Cryptography Function	Algorithms Supported in Cisco BAC
Encryption types	• DES The Data Encryption Standard applies a 56-bit key to each 64-bit block of data. This key is used for encryption and decryption. • 3DES or Triple DES The Triple-Strength Data Encryption Standard in case DES is used with three keys. • RC4 The Rivest Cipher 4 which is a variable key-size stream cipher used for file encryption.
Message authentication algorithms	• MD5 (Message Digest 5) The algorithm used in digital signature applications to produce a 128-bit message digest, which is unique to the message and can be used to verify data integrity. • Secure Hash Algorithm (SHA) The algorithm used in the Digital Signature Standard to produce a 160-bit hash value.

Caution The dh-anon series of cipher suites are intended for completely anonymous Diffie-Hellman communications in which neither party is authenticated. Note that this cipher suite is vulnerable to attacks.

Cipher suites with “export” in the title indicate that they are intended for use outside the United States. These cipher suites have encryption algorithms with limited key sizes, for example, 3DES or RC4 with 128-bit encryption.

Table 6-6 Cipher Suites Supported in BAC

Cipher Suite	Exportable	Key Exchange Algorithm Used
all-cipher-suites	No	EDH *
ssl_dh_anon_export_with_des40_cbc_sha	Yes	DH **
ssl_dh_anon_with_des_cbc_sha	No	DH **
ssl_dh_anon_export_with_rc4_40_md5	Yes	DH **
ssl_dh_anon_with_3des_ede_cbc_sha	No	DH **
ssl_dhe_dss_with_des_cbc_sha	No	DH **
ssl_dh_anon_with_rc4_128_md5	No	DH **
ssl_dhe_dss_export_with_des40_cbc_sha	Yes	EDH *
ssl_dhe_dss_with_3des_ede_cbc_sha	No	EDH *

Table 6-6 Cipher Suites Supported in BAC (continued)

Cipher Suite	Exportable	Key Exchange Algorithm Used
ssl_dhe_rsa_export_with_des40_cbc_sha	Yes	EDH *
ssl_dhe_rsa_with_3des_ede_cbc_sha	No	EDH *
ssl_dhe_rsa_with_des_cbc_sha	No	EDH *
ssl_rsa_export_with_des40_cbc_sha	Yes	RSA
ssl_rsa_export_with_rc4_40_md5	Yes	RSA
ssl_rsa_with_3des_ede_cbc_sha	No	RSA
ssl_rsa_with_des_cbc_sha	No	RSA
ssl_rsa_with_null_md5	No	RSA
ssl_rsa_with_null_sha	No	RSA
ssl_rsa_with_rc4_128_md5	No	RSA
ssl_rsa_with_rc4_128_sha	No	RSA
tls_dh_anon_with_aes_128_cbc_sha	No	DH **
tls_dhe_dss_with_aes_128_cbc_sha	No	EDH *
tls_dhe_rsa_with_aes_128_cbc_sha	No	EDH *
tls_rsa_with_aes_128_cbc_sha	No	RSA

```
* refers to the Ephemeral Diffie-Hellman algorithm
** refers to the Diffie-Hellman algorithm.
```

CHAPTER 7

SNMP Agent Commands

This chapter describes the command line interface (CLI) commands that you can use to manage and monitor the SNMP agent in the Cisco Broadband Access Center (Cisco BAC) Device Provisioning Engine (DPE).

The commands described in this chapter are:

snmp-server community

Use this command to set up the community access string to allow access for external SNMP managers to the DPE SNMP agent.

After you use this command, run the **snmp-server reload** command to restart the SNMP agent. See snmp-server reload, page 7-6, for additional information.

To delete a specified community string, use the **no** form of this command (see no snmp-server community, page 7-2).

Syntax Description

snmp-server 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 NMS and the managed device must reference the same community string.
- **rw**—Assigns a read-write (rw) community string. SNMP applications require rw access for Set operations. The rw community string enables write access to 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.

Examples

```
dpe# snmp-server community test_community ro
% OK ()
Requires SNMP agent restart "# snmp-server reload"
```

no snmp-server community

Use this command to delete the specified community string.

After you use this command, run the **snmp-server reload** command to restart the SNMP agent. See snmp-server reload, page 7-6, for additional information.

To set up the community access string to allow access for external SNMP managers to the DPE SNMP agent, use the **snmp-server community** command. See snmp-server community, page 7-1, for more information.

Syntax Description

no snmp-server community *string*

string—Identifies the SNMP community.

Examples

```
dpe# no snmp-server community test_community
% OK ()
Requires SNMP agent restart "# snmp-server reload"
```

snmp-server contact

Use this command to enter a string of characters that identify the system contact (sysContact) as defined in the MIB II.

After you use this command, run the **snmp-server reload** command to restart the SNMP agent. See snmp-server reload, page 7-6, for additional information.

To remove the system contact that was responsible for the DPE, use the **no** form of this command. See no snmp-server contact, page 7-3, for more information.

Syntax Description

snmp-server contact *text*

text—Identifies the name of the contact responsible for the DPE.

Examples

```
dpe# snmp-server contact joe
% OK (Requires SNMP server restart "# snmp-server reload")
```

no snmp-server contact

Use this command to remove the system contact that was responsible for the DPE.

After you use this command, run the **snmp-server reload** command to restart the SNMP agent. See snmp-server reload, page 7-6, for additional information.

To enter a string of characters that identify the system contact, use the **snmp-server contact** command. See snmp-server contact, page 7-2, for more information.

Syntax Description

No keywords or arguments.

Examples

```
dpe# no snmp-server contact
% OK (Requires SNMP server restart "# snmp-server reload")
```

snmp-server host

Use this command to specify the recipient of all SNMP notifications. It is possible to use multiple instances of this command to specify more than one notification recipient.

After you use this command, run the **snmp-server reload** command to restart the SNMP agent. See snmp-server reload, page 7-6, for additional information.

To remove the specified notification recipient, use the **no** form of this command. See no snmp-server host, page 7-4, for more information.

Syntax Description

snmp-server host *host-addr* **notification community** *community* **udp-port** *port*

- *host-addr*—Specifies the IP address of the host to which notifications are sent.
- *community*—Specifies the community string to use while sending SNMP notifications.
- *port*—Identifies the UDP port used to send SNMP notifications. The default UDP port number is 162.

Examples

```
dpe# snmp-server host 10.10.10.5 notification community public udp-port 162
% OK ()
Requires SNMP agent restart "# snmp-server reload"
```

no snmp-server host

Use this command to remove the specified notification recipient.

After you use this command, run the **snmp-server reload** command to restart the SNMP agent. See snmp-server reload, page 7-6, for additional information.

To specify the recipient of all SNMP notifications, use the **snmp-server host** command. See snmp-server host, page 7-3, for more information.

Syntax Description

no snmp-server host *host-addr* **notification**

host-addr—Identifies the IP address of the host

Examples

```
dpe# no snmp-server host 10.10.10.5 notification
% OK ()
Requires SNMP agent restart "# snmp-server reload"
```

snmp-server inform

Use this command to specify the type of SNMP notification sent, from the SNMP agent, to the SNMP manager. Use it to send SNMP informs instead of traps; although traps are sent by default.

After you use this command, run the **snmp-server reload** command to restart the SNMP agent. See snmp-server reload, page 7-6, for additional information.

To switch the SNMP notifications back to the default setting of traps, use the **no** form of this command. See no snmp-server inform, page 7-5, for more information.

Syntax Description

snmp-server inform [**retries** *count* **timeout** *time*]

- *count*—Identifies the number of times that an inform can be sent from the SNMP agent to the manager. If the timeout period expires before the configured number of retries is reached, the SNMP server will cease sending informs.
- *time*—Identifies the length of time (in milliseconds) that the SNMP server will continue sending informs. If the maximum number of retries is reached before the timeout expires, the SNMP server will cease sending informs.

Note Specification of the retry count and timeout, while configuring SNMP informs, is optional. If not specified, the default values of 1 retry and 5000 milliseconds are used.

Examples

```
dpe# snmp-server inform retries 5 timeout 500
% OK ()
Requires SNMP server restart "# snmp-server reload"
```

From this example, an SNMP inform will be sent up to a maximum of 5 times, before the retries stop. If the timeout of 500 milliseconds expires before the 5 retries takes place, the inform is not sent again.

no snmp-server inform

Use this command to switch the SNMP notifications that are sent to the SNMP manager, back to the default setting of traps.

To specify the type of SNMP notification sent, use the **snmp-server inform** command. See snmp-server inform, page 7-4, for more information.

Syntax Description No keywords or arguments.

Examples

```
dpe# no snmp-server inform
% OK
```

snmp-server location

Use this command to enter a string of characters that identify the system location (sysLocation) as defined in the MIB II.

After you use this command, run the **snmp-server reload** command to restart the SNMP agent. See snmp-server reload, page 7-6, for additional information.

To remove a system location, use the **no** form of this command. See no snmp-server location, page 7-5, for more information.

Syntax Description **snmp-server location** *text*

text—Identifies the physical location of the DPE.

Examples

```
dpe# snmp-server location st_louis
% OK (Requires SNMP server restart "# snmp-server reload")
```

no snmp-server location

Use this command to remove a system location.

After you use this command, run the **snmp-server reload** command to restart the SNMP agent. See snmp-server reload, page 7-6, for additional information.

To enter a string of characters that identify the system location, use the **snmp-server location** command. See snmp-server location, page 7-5, for more information.

Syntax Description No keywords or arguments.

Examples

```
dpe# no snmp-server location
% OK (Requires SNMP server restart "# snmp-server reload")
```

snmp-server reload

Use this command to reload the SNMP agent process on the DPE. After this command is entered the SNMP agent processes that are reloaded, appear.

When the SNMP process is started on the RDU and DPE, a trap containing the system uptime is sent. However, Cisco BAC trap notifications, are disabled by default. You can only enable trap notifications by setting the corresponding MIB object using SNMP. You cannot enable trap notification using the CLI or the administrator user interface.

This Cisco BAC release supports only the trap notifications defined in the CISCO-BACC-SERVER-MIB file. For more information, refer to the MIB files under the *BPR_HOME/rdu/mibs* directory.

Syntax Description

No keywords or arguments.

Examples

```
dpe# snmp-server reload
Process snmpAgent has been restarted
dpe#
```

snmp-server start | stop

Use this command to start or stop the SNMP agent process on the DPE.

Syntax Description

snmp-server start | **stop**

- **start**—Starts the SNMP agent process on the DPE.

  Note Use this command only when the SNMP agent is not running. If you run this command when the SNMP agent is already running, the following message appears:

  ```
  Process snmpAgent is already running
  ```

- **stop**—Stops the SNMP agent process on the DPE.

Examples

Example 1

```
dpe# snmp-server start
Process snmpAgent has been started
% OK
```

Example 2

```
dpe# snmp-server stop
Process snmpAgent has been stopped
dpe#
```

snmp-server udp-port

Use this command to identify the UDP port number to which the SNMP agent listens.

The DPE requires this command to prevent potential sharing violations between ports that other applications use. The changing of port numbers is used to resolve potential port conflict.

The SNMP agent's default port number, 8001, is different from the standard well-known SNMP agent port to eliminate potential port conflicts with other SNMP agents on the Solaris computer.

Note We recommend that you change the UDP port to the well-known port, number 161, for the SNMP agent.

To change the port to which the SNMP agent listens back to the default UDP port number, use the **no** form of this command. See no snmp-server udp-port, page 7-7, for more information.

Syntax Description

snmp-server udp-port *port*

port—Identifies the UDP port to which the SNMP agent listens.

Examples

```
dpe# snmp-server udp-port 161
% OK
```

no snmp-server udp-port

Use this command to change the port to which the SNMP agent listens back to the default UDP port number (8001).

Note Using a port number other than the standard, well-known SNMP agent port number of 161 may increase the likelihood of potential port conflicts with other SNMP agents running on the same Solaris computer.

To identify the UDP port number to which the SNMP agent listens, use the **snmp-server udp-port** command. See snmp-server udp-port, page 7-7, for more information.

Syntax Description

No keywords or arguments.

Examples

```
dpe# no snmp-server udp-port
% OK
```

CHAPTER 8

Log and Debug Commands for DPE

This chapter describes the command line interface (CLI) commands that you can use to debug the Cisco Broadband Access Center (Cisco BAC) Device Provisioning Engine (DPE), and monitor and manage the Cisco BAC log system.

Note Before using any debug command, ensure that DPE debugging is enabled. Run the **debug on** command to enable this function. See debug on, page 8-5, for more information.

The commands described in this section are:

clear logs

Use this command to remove historic (out-of-date) log files that exist on the system. These files include:

- DPE logs
- Syslog

Over time, historic log files accumulate in the DPE. The **support bundle state** command is used to bundle these logs. We recommend that you create a bundle before clearing logs to ensure that no necessary files are accidently lost.

After you enter this command, prompts appear to indicate that logs are being cleared. The number of log files that are cleared, is also identified.

Examples

```
dpe# clear logs
Clearing historic log files...
+ Removing 1 DPE log files...
+ No more historic logs.
```

debug dpe

The **debug dpe** is the global syntax of the commands that you use to debug the various services on the DPE.

Note If you run the following commands on an unlicensed DPE, a message similar to this one appears:

```
This DPE is not licensed. Your request cannot be serviced.
Please check with your system administrator for DPE licenses.
```

Table 8-1 describes the various commands you can use to debug the DPE.

Table 8-1 List of debug dpe Commands

Command Usage	Example
debug dpe cache **no debug dpe cache**	
Enables you to debug DPE cache logging, which involves messages pertaining to the DPE cache including: • Logging requests for cache entries. • Updates to the cache. • Other interactions by DPE subsystems. To disable DPE cache debug logging, use the **no** form of this command.	dpe# **debug dpe cache** % OK
debug dpe chatty-client **no debug dpe chatty-client**	

Table 8-1 List of debug dpe Commands (continued)

Command Usage	Example
Enables you to debug the chatty-client service, which logs chatty-client service status and error messages. To disable the debugging of the chatty-client service, use the **no** form of this command.	dpe# **debug dpe chatty-client** % OK
debug dpe connection **no debug dpe connection**	
Enables you to debug the DPE connection, which logs communication subsystem status and error messages. Use this command for finding communication problems between the DPE and the RDU. To disable the debugging of the DPE connection, use the **no** form of this command.	dpe# **debug dpe connection** % OK
debug dpe dpe-ext **no debug dpe dpe-ext**	
Enables you to debug the DPE extensions, which involves logging messages about the overall status and issues of the DPE extensions. To disable debugging of the DPE extensions, use the **no** form of this command.	dpe# **debug dpe dpe-ext** % OK
debug dpe dpe-server **no debug dpe dpe-server**	
Enables you to debug the DPE server, which involves logging messages about the overall status and issues of the DPE server. To disable debugging of the DPE server, use the **no** form of this command.	dpe# **debug dpe dpe-server** % OK
debug dpe event-manager **no debug dpe event-manager**	
Enables you to debug the DPE event manager, which involves logging messages and conditions showing the state of the event manager. To disable debugging of the DPE event manager, use the **no** form of this command. Debugging of the DPE event manager is, by default, enabled.	dpe# **debug dpe event-manager** % OK

Table 8-1 List of debug dpe Commands (continued)

Command Usage	Example
debug dpe exceptions **no debug dpe exceptions**	
Enables you to debug the DPE exceptions, which involves logging full stack traces for exceptions occurring during system operation. When unusual situations occur, where the system is apparently corrupt or behaving abnormally, running this command can reveal valuable information for the Cisco TAC support. To disable the debugging of DPE exceptions, use the **no** form of this command. Debugging of DPE exceptions is, by default, enabled.	dpe# **debug dpe exceptions** % OK
debug dpe framework **no debug dpe framework**	
Enables you to debug the DPE framework, which involves logging information about the DPE server's underlying framework. This underlying infrastructure provides support for all of the various servers in Cisco BAC. To disable the debugging of the DPE framework, use the **no** form of this command. Debugging of the DPE framework is, by default, enabled.	dpe# **debug dpe framework** % OK
debug dpe messaging **no debug dpe messaging**	
Enables you to debug the DPE messaging, which involves logging details about the DPE messaging subsystem. This subsystem is used primarily for communication between the DPE and the RDU. To disable the debugging of DPE messaging, use the **no** form of this command.	dpe# **debug dpe messaging** % OK
debug dpe statistics **no debug dpe statistics**	
Enables you to collect the performance statistics. To disable debugging of the DPE performance statistics collection, use the **no** form of this command.	dpe# **debug dpe statistics** % OK

debug on

Use this command to enable debug logging, which can be helpful when troubleshooting possible system problems. Additionally, specific debugging categories must be enabled separately with commands such as **debug dpe cache**.

To disable debug logging, run the **no debug** command. See no debug, page 8-5, for more information.

Caution Enabling debug logging may have a severe impact on DPE performance. The DPE should never be left running with debug turned on for long periods of time.

If you run this command on an unlicensed DPE, a message similar to this one appears:

```
This DPE is not licensed. Your request cannot be serviced.
Please check with your system administrator for DPE licenses.
```

Defaults

Debug logging is, by default, enabled.

Examples

```
dpe# debug on
% OK
```

no debug

Use this command to disable all debug logging.

If you run this command on an unlicensed DPE, a message similar to this one appears:

```
This DPE is not licensed. Your request cannot be serviced.
Please check with your system administrator for DPE licenses.
```

To enable debugging, use the **debug on** command. For more information, see debug on, page 8-5.

Examples

```
dpe# no debug
% OK
```

log level

Use this command to set the level of minimum DPE log messages that will be saved, as described in the *Cisco Broadband Access Center Administrator's Guide, Release 3.5, 3.5.1, 3.5.2*.

If you run this command on an unlicensed DPE, a message similar to this one appears:

```
This DPE is not licensed. Your request cannot be serviced.
Please check with your system administrator for DPE licenses.
```

Syntax Description

```
log level number
```

number—Identifies the logging level, by number, to be saved. The log levels that Cisco BAC supports are described in Table 8-2.

Table 8-2 DPE Log Levels

Log Level No.	Description
0-emergency	Saves all emergency messages
1-alert	Saves all activities that need immediate action and those of a more severe nature
2-critical	Saves all critical conditions and those of a more severe nature
3-error	Saves all error messages and those of a more severe nature
4-warning	Saves all warning messages and those of a more severe nature
5-notification	Saves all notification messages and those of a more severe nature
6-info	Saves all logging messages available

Setting a specific log level saves messages less than or equal to the configured level. For example, when you set the log level at 5-notification, all events generating messages with a log level of 4 or less are written into the log file.

The logging system's log levels are used to identify the urgency with which you might want to address log issues. The 0-emergency setting is the most severe level of logging while 6-info is the least severe, saving mostly informational log messages.

Defaults

The level of minimum DPE log messages that will be saved is, by default, set at 5-notification.

Examples

```
dpe# log level 6
% OK
```

show log

Use this command to show all recent log entries for the DPE. These logs contain general DPE process information, including logging all system errors or severe problems. Check this log when the system is experiencing difficulties. If the log contains insufficient information, enable the debug logging function and experiment with the different categories related to the problem.

Syntax Description

```
show log [last 1..999 | run]
```

- **last** *1..999*—Shows the specified number of recent log entries for the DPE, with *1..999* specifying the number of log entries that you want to display. This element is optional.
- **run**—Displays the running DPE log, which starts showing all messages logged to the DPE log. The command continues to run until you press Enter. This element is optional.

Examples

Example 1

```
dpe# show log
2006 02 14 07:50:26 EST: %BAC-DPE-7-DEBUG_FRAMEWORK: ThreadMonitor:
BACThread[Connector,5,BAC,alive]
```

Note The output of this command has been shortened for demonstration purposes.

Example 2

```
dpe# show log last 3
2006 02 14 07:51:26 EST: %BAC-DPE-7-DEBUG_FRAMEWORK: ThreadMonitor:     Cwmp1Thread-1
2006 02 14 07:51:26 EST: %BAC-DPE-7-DEBUG_FRAMEWORK: ThreadMonitor:     Http1Thread-0
2006 02 14 07:51:26 EST: %BAC-DPE-7-DEBUG_FRAMEWORK: ThreadMonitor:     Http1Thread-1
```

Example 3

```
dpe# show log run
% Press <enter> to stop.
2006 02 14 07:53:22 EST: %BAC-DPE-7-DEBUG_FRAMEWORK: OSStatusService: current CPU load
percentage 1%
2006 02 14 07:53:25 EST: %BAC-DPE-7-DEBUG_FRAMEWORK: MemoryMonitor: Memory:
2006 02 14 07:53:25 EST: %BAC-DPE-7-DEBUG_FRAMEWORK: MemoryMonitor: Total memory 29777920
2006 02 14 07:53:25 EST: %BAC-DPE-7-DEBUG_FRAMEWORK: MemoryMonitor: Free memory 4058120
2006 02 14 07:53:26 EST: %BAC-DPE-7-DEBUG_FRAMEWORK: ThreadMonitor: Threads:

Stopped.
```

CHAPTER 9

Debug Commands for CWMP Technology

This chapter describes the command line interface (CLI) commands that you can use to debug the CWMP technology on the Cisco Broadband Access Center (Cisco BAC) Device Provisioning Engine (DPE).

Note Before using any debug command, ensure that DPE debugging is enabled by running the **debug on** command. See debug on, page 8-5, for more information.

The commands described in this chapter are:

debug service *type*

This is the global syntax of the commands that you use to debug the CWMP service and the HTTP file service that run on the DPE.

Syntax Description

```
debug service type num
```

- *type*—Specifies the service, which could be CWMP or HTTP.
  - CWMP—Enables you to debug the CWMP service on the DPE.
  - HTTP—Enables you to debug the HTTP file service on the DPE.
- *num*—Specifies the instance of the service, which could be 1 or 2.

For a list of commands used to debug the CWMP service, see debug service cwmp, page 9-2.

For a list of commands used to debug the HTTP file service, see debug service http, page 9-9.

debug service cwmp

This section describes the commands that you use to debug the CWMP service that runs on the DPE.

Note Before using any debug commands that follow, ensure that DPE debugging is enabled. Run the **debug on** command to enable this function. See debug on, page 8-5, for more information.

Syntax Description

debug service cwmp *num*

num—Specifies the instance of the service, which could be 1 or 2.

Table 9-1 describes the commands that you can use to debug the CWMP service.

Table 9-1 List of debug service cwmp Commands

Command Usage	Example
debug service cwmp *num* client-auth-all **no debug service cwmp *num* client-auth-all**	
Enables detailed debugging of successful and failed client authentication, for the CWMP service. To disable detailed debugging of successful and failed authentication for the CWMP service, use the **no** form of this command.	dpe# **debug service cwmp 1 client-auth-all** % OK
debug service cwmp *num* client-auth-failures **no debug service cwmp *num* client-auth-failures**	
Enables detailed debugging of failed client authentication for the CWMP service. To disable detailed debugging of failed client authentication for the CWMP service, use the **no** form of this command.	dpe# **debug service cwmp 1 client-auth-failures** % OK
debug service cwmp connection-request-service **no debug service cwmp connection-request-service**	
Enables debugging of the CWMP connection request service, involving requests from the DPE to the CPE device. To disable debugging of the CWMP connection request service, use the **no** form of this command. **Note** You need not mention the CWMP instance for this command.	dpe# **no debug service cwmp connection-request-service** % OK
debug service cwmp *num* cpe-config-sync **no debug service cwmp *num* cpe-config-sync**	
Enables detailed debugging of the device configuration synchronization, involving DPE interactions with the CPE device, for the CWMP service. To disable detailed debugging of the CWMP device configuration synchronization service, use the **no** form of this command.	dpe# **debug service cwmp 1 cpe-config-sync** % OK

Table 9-1 List of debug service cwmp Commands (continued)

Command Usage	Example
debug service cwmp *num* cpe-signed-config-sync **no debug service cwmp *num* cpe-signed-config-sync**	
Enables detailed debugging of the device signed configuration synchronization for the CWMP service. To disable detailed debugging of the device signed configuration synchronization service, use the **no** form of this command.	dpe# **debug service cwmp 1 cpe-signed-config-sync** % OK
debug service cwmp *num* data-sync **no debug service cwmp *num* data-sync**	
Enables detailed debugging of data synchronization in interactions between the RDU and the CPE. This data relates to device discovery and device updates that are forwarded to the RDU. To disable detailed debugging of the data synchronization service, use the **no** form of this command.	dpe# **debug service cwmp 1 data-sync** % OK
debug service cwmp *num* device-operations **no debug service cwmp *num* device-operations**	
Enables debugging the execution of device operations on the DPE. To disable debugging the execution of device operations on the DPE, use the **no** form of this command.	dpe# **debug service cwmp 1 device-operations** % OK
debug service cwmp device-operations-cache **no debug service cwmp device-operations-cache**	
Enables debugging of the immediate-mode device operation cache that all CWMP services use. To disable debugging of the immediate-mode device operation cache that all CWMP services use, use the **no** form of this command. **Note** You need not mention the CWMP instance for this command.	dpe# **debug service cwmp device-operations-cache** % OK

Table 9-1 List of debug service cwmp Commands (continued)

Command Usage	Example
debug service cwmp *num* errors **no debug service cwmp *num* errors**	
Enables debugging of low-level errors generated during interactions involving the CWMP service running on the DPE. These errors are not usually logged. To disable debugging of low-level errors generated during interaction involving the CWMP service, use the **no** form of this command.	dpe# **debug service cwmp 1 errors** % OK
debug service cwmp *num* extension **no debug service cwmp *num* extension**	
Enables debugging of the service extensions for the CWMP service running on the DPE. To disable debugging of the service extensions for the CWMP service, use the **no** form of this command.	dpe# **debug service cwmp 1 extension** % OK
debug service cwmp *num* firmware **no debug service cwmp *num* firmware**	
Enables debugging the execution of firmware rules for the CWMP service. These rules include messages and conditions that detail the state of the device firmware. To disable debugging the execution of firmware rules for the CWMP service, use the **no** form of this command.	dpe# **debug service cwmp 1 firmware** % OK
debug service cwmp *num* http-details **no debug service cwmp *num* http-details**	
Enables debugging of low-level details for the CWMP service running on the DPE. To disable debugging of low-level details for the CWMP service, use the **no** form of this command.	dpe# **debug service cwmp 1 http-details** % OK
debug service cwmp *num* http-faults **no debug service cwmp *num* http-faults**	
Enables debugging of the error responses generated during interactions involving the CWMP service running on the DPE. To disable debugging of the error responses generated during interactions involving the CWMP service, use the **no** form of this command.	dpe# **debug service cwmp 1 http-faults** % OK

Table 9-1 List of debug service cwmp Commands (continued)

Command Usage	Example
debug service cwmp *num* http-headers **no debug service cwmp *num* http-headers**	
Enables detailed debugging of the request and response headers for the CWMP service. To disable detailed debugging of the request and response headers for the CWMP service, use the **no** form of this command.	dpe# **debug service cwmp 1 http-headers** % OK
debug service cwmp *num* http-requests **no debug service cwmp *num* http-requests**	
Enables detailed debugging of the requests in the payload of a message for the CWMP service. To disable detailed debugging of the requests in the payload of a message for the CWMP service, use the **no** form of this command.	dpe# **debug service cwmp 1 http-requests** % OK
debug service cwmp *num* http-responses **no debug service cwmp *num* http-responses**	
Enables detailed debugging of the responses in the payload of a message for the CWMP service. To disable detailed debugging of the responses in the payload of a message for the CWMP service, use the **no** form of this command.	dpe# **debug service cwmp 1 http-responses** % OK
debug service cwmp *num* instr-gen-requests **no debug service cwmp *num* instr-gen-requests**	
Enables debugging of the instruction generation requests for the CWMP service involving interactions with the CPE. To disable debugging of the instruction generation requests, use the **no** form of this command.	dpe# **debug service cwmp 1 instr-gen-requests** % OK
debug service cwmp *num* instruction-details **no debug service cwmp *num* instruction-details**	
Enables detailed debugging of the instruction processing for the CWMP service involving interactions with the CPE. To disable detailed debugging of the instruction processing for the CWMP service, use the **no** form of this command.	dpe# **debug service cwmp 1 instruction-details** % OK

Table 9-1 List of debug service cwmp Commands (continued)

Command Usage	Example
debug service cwmp *num* instruction-lookup **no debug service cwmp *num* instruction-lookup**	
Enables debugging of the DPE instruction lookup details for the CWMP service involving interactions with the CPE. To disable debugging of the DPE instruction lookup details for the CWMP service, use the **no** form of this command.	dpe# **debug service cwmp 1 instruction-lookup** % OK
debug service cwmp *num* instruction-rpc **no debug service cwmp *num* instruction-rpc**	
Enables debugging of the RPC instruction processing for the CWMP service involving interactions with the CPE. To disable debugging of the RPC instruction processing for the CWMP service, use the **no** form of this command.	dpe# **debug service cwmp 1 instruction-rpc** % OK
debug service cwmp *num* instruction-states **no debug service cwmp *num* instruction-states**	
Enables debugging of instruction state transitions during instruction processing for the CWMP service. To disable debugging of instruction state transitions during instruction processing for the CWMP service, use the **no** form of this command.	dpe# **debug service cwmp 1 instruction-states** % OK
debug service cwmp *num* ipe **no debug service cwmp *num* ipe**	
Enables debugging of the DPE instruction processing engine execution for the CWMP service. To disable debugging of the DPE instruction processing engine execution for the CWMP service, use the **no** form of this command.	dpe# **debug service cwmp 1 ipe** % OK
debug service cwmp *num* session **no debug service cwmp *num* session**	
Enables debugging the lifecycle of a CWMP session between the DPE and the CPE device. To disable debugging of the CWMP session, use the **no** form of this command.	dpe# **debug service cwmp 1 session** % OK

Table 9-1 List of debug service cwmp Commands (continued)

Command Usage	Example
debug service cwmp session-manager **no debug service cwmp session-manager**	
Enables debugging of the session manager for the CWMP service that is responsible for managing sessions. To disable debugging of the session manager for the CWMP service, use the **no** form of this command. **Note** You need not mention the CWMP instance for this command.	dpe# **debug service cwmp session-manager** % OK
debug service cwmp *num* soap-faults **no debug service cwmp *num* soap-faults**	
Enables the debugging of all SOAP faults, received and sent, for the CWMP service involving interactions with the CPE device. To disable debugging of all SOAP faults for the CWMP service, use the **no** form of this command.	dpe# **debug service cwmp 1 soap-faults** % OK
debug service cwmp *num* soap-informs **no debug service cwmp *num* soap-informs**	
Enables debugging of all received Inform messages for the CWMP service in interactions between the DPE and the CPE device. To disable debugging of all received Inform messages for the CWMP service, use the **no** form of this command.	dpe# **debug service cwmp 1 soap-informs** % OK
debug service cwmp *num* unknown-devices **no debug service cwmp *num* unknown-devices**	
Enables debugging the processing of device configurations that are not stored in the DPE cache. To disable debugging the processing of device configurations not stored in the DPE cache, use the **no** form of this command.	dpe# **debug service cwmp 1 unknown-devices** % OK

Table 9-1 List of debug service cwmp Commands (continued)

Command Usage	Example
debug service cwmp-redirect **no debug service cwmp-redirect**	
Enables the DPE to debug the home provisioning group redirection operations. To disable debugging of the home provisioning group redirection operations, use the **no** form of this command. You need not restart the DPE for this command to take effect.	`dpe# debug service cwmp-redirect` `% OK`

debug service http

This section describes the commands that you use to debug the HTTP file service that runs on the DPE.

Note Before using any debug command, ensure that DPE debugging is enabled. Run the **debug on** command to enable this function. See debug on, page 8-5, for more information.

Syntax Description

debug service http *num*

num—Specifies the instance of the service, which could be 1 or 2.

Table 9-2 describes the commands that you can use to debug the HTTP file service.

Table 9-2 List of debug service http Commands

Command Usage	Example
debug service http *num* client-auth-all **no debug service http *num* client-auth-all**	
Enables debugging of successful and failed client authentication for the HTTP service. To disable debugging of successful and failed client authentication for the HTTP service, use the **no** form of this command.	`dpe# debug service http 1 client-auth-all` `% OK`

Table 9-2 List of debug service http Commands (continued)

Command Usage	Example
debug service http *num* client-auth-failures **no debug service http *num* client-auth-failures**	
Enables debugging of client authentication failures for the HTTP service. To disable debugging of client authentication failures of the HTTP service, use the **no** form of this command.	dpe# **debug service http 1 client-auth-failures** % OK
debug service http *num* details **no debug service http *num* details**	
Enables debugging the low-level details of the HTTP service running on the DPE. To disable debugging the low-level details of the HTTP service, use the **no** form of this command.	dpe# **debug service http 1 details** % OK
debug service http *num* errors **no debug service http *num* errors**	
Enables debugging of request errors for the HTTP service running on the DPE. To disable debugging of request errors for the HTTP service, use the **no** form of this command.	dpe# **debug service http 1 errors** % OK
debug service http *num* faults **no debug service http *num* faults**	
Enables debugging of the error responses of the HTTP service running on the DPE. To disable debugging of the error responses of the HTTP service, use the **no** form of this command.	dpe# **debug service http 1 faults** % OK
debug service http *num* headers **no debug service http *num* headers**	
Enables debugging of the request and response headers for the HTTP service running on the DPE. To disable debugging of the request and response headers for the HTTP service, use the **no** form of this command.	dpe# **debug service http 1 headers** % OK

Table 9-2 List of debug service http Commands (continued)

Command Usage	Example
debug service http *num* request-processing **no debug service http *num* request-processing**	
Enables debugging of successful and failed request processing, for the HTTP service running on the DPE. To disable debugging of successful and failed request processing for the HTTP service, use the **no** form of this command.	dpe# **debug service http 1 request-processing** % OK
debug service http framework **no debug service http framework**	
Enables debugging of the HTTP framework activity that is not associated with a particular service. To disable debugging of the HTTP framework activity, use the **no** form of this command. **Note** You need not specify the HTTP instance for this command.	dpe# **debug service http framework** % OK

debug service ssl

Use this command to enable debugging of the process accepting a SSL/TLS connection in CWMP exchanges between the DPE and the CPE device.

To disable debugging of the process accepting a SSL/TLS connection, use the **no** form of this command.

When using this command, you must restart the DPE for the changes to take effect. To restart the DPE, run the **dpe reload** command. Refer to dpe reload, page 3-5, for more information.

Examples

```
dpe# debug service ssl
% OK (Requires DPE restart "# dpe reload")
```

CHAPTER 10

Support and Troubleshooting Commands

This chapter contains the command line interface (CLI) commands that you can use to provide troubleshooting support for the Cisco Broadband Access Center (Cisco BAC) Device Provisioning Engine (DPE).

The commands described in this chapter are:

clear bundles

Use this command to clear any existing archived bundles on the DPE. You create these bundles by using the **support bundle** commands. These commands normally contain archived logs and archived state information that Cisco Technical Assistance Center (TAC) uses

Note Before using this command, ensure that all bundles are retrieved because the archived state is lost.

After you enter the command, a prompt appears to indicate that the bundles are being cleared and, when this is complete, the amount of disk space cleared (in bytes) appears.

Syntax Description

No keywords or arguments.

Examples

Example 1

```
dpe# clear bundles
Clearing Cisco support bundles...
+ 10101760 bytes cleared.
```

This result occurs when existing archived bundles are cleared.

Example 2

```
dpe# clear bundles
Clearing Cisco support bundles...
+ No bundles to clear.
```

This result occurs when there are no archived bundles to clear.

show bundles

Use this command to display the bundles currently available in the outgoing directory. You create these bundles by using the **support bundle** commands.

This command identifies the bundles that are archived. If there are no bundles, a prompt appears , indicating that there are no bundles available.

Syntax Description

No keywords or arguments.

Examples

Example 1

```
dpe# show bundles
outgoing/cache-20060214-002023.bac
outgoing/state-20060214-002230.bac
```

This result occurs when bundles are currently archived.

Example 2

```
dpe# show bundles
No bundles currently available.
```

This result occurs when there are no bundles currently archived.

support bundle cache

Use this command to bundle the current DPE cache. This command helps to you to archive the cache to send it to the Cisco TAC. After the bundle is created, it is available from the outgoing directory of the FTP server.

After the command is entered, a cache bundle is created for use by the TAC. The command displays the bundle specifics, including the compressed size of the bundle file.

Syntax Description

No keywords or arguments.

Examples

```
dpe# support bundle cache
Creating cache bundle for Cisco support...
+ outgoing/cache-20060721-000218.bac
+ Adding & compressing DPE cache...
+ Size: 11780584 bytes
```

support bundle state

Use this command to bundle the current DPE state. This command helps you to archive configuration and log files to send them to the Cisco TAC. After the bundle is created, it is available from the outgoing directory of FTP server.

When sending information to the Cisco TAC, you should send the DPE bundle obtained with this command, and the state bundle obtained at the RDU. You generate this bundle by running the **bundleState.sh** command from the *BPR_HOME*/rdu/bin directory.

A script *BPR_HOME*/rdu/bin/bundlestate is available on the RDU. You use this script to bundle the RDU system state, including logs, when sending information to the TAC.

After the command is entered, the current state of the DPE is bundled together; then the bundle file is compressed and identified for TAC use.

Syntax Description

No keywords or arguments.

Examples

```
dpe# support bundle state
Creating state bundle for Cisco support...
+ /outgoing/state-20060721-000340.bac
+ Adding a process listing to the support bundle...
+ Adding a network connection listing to the support bundle...
+ Adding and compressing files for support bundle...
+ Size: 1205782 bytes
```

GLOSSARY

A

alert — A syslog or SNMP message notifying an operator or administrator of a problem.

API — Application programming interface. Specification of function-call conventions that defines an interface to a service.

audit logs — A log file containing a summary of major changes in the RDU database. This includes changes to system defaults, technology defaults, and classes of service.

B

broadband — Transmission system that multiplexes multiple independent signals onto one cable. In Telecommunication terminology, any channel having a bandwidth greater than a voice-grade channel (4 kHz). In LAN terminology, a coaxial cable on which to use analog signaling.

Cisco Broadband Access Center (BAC) — An integrated solution for broadband service providers to provision and manage subscriber-edge services by using the DSL Forum's CPE WAN Management Protocol, a standard defined in the TR-069 specification. BAC is a scalable product capable of supporting millions of devices.

C

caching — Form of replication in which information learned during a previous transaction is used to process subsequent transactions.

cipher suites — Provide cryptographic algorithms that the SSL module requires to perform key exchange, authentication, and Message Authentication Code.

customer premises equipment (CPE) — Terminating equipment, such as telephones, computers, and modems, supplied and installed at a customer location.

CPE WAN Management Protocol (CWMP) — A standard defined in the TR-069 specification by the DSL Forum. CWMP integrates the capabilities defined in TR-069 to increase operator efficiency and reduce network management problems.

D

debug An operation designed to aid in debugging another program by allowing the administrator to step through the program, examine the data, and monitor conditions, such as the values of variables.

device provisioning engine (DPE) Device Provisioning Engine servers cache device instructions and perform CWMP services. These distributed serves automatically synchronize with the RDU to obtain the latest instructions and provide BAC scalability.

F

fully qualified domain name (FQDN) Fully qualified domain name. FQDN is the full name of a system, rather than just its hostname. For example, cisco is a hostname and www.cisco.com is an FQDN.

I

instruction generation The process of generating policy instructions at the RDU for devices and distributing these instructions to the DPE. The instructions are cached by the DPE and informed about an action to be performed on the CPE. This action may include configuration, firmware upgrade, or other operations.

IP address An IP address is a 32-bit number that identifies each sender or receiver of information that is sent in packets across the Internet.

N

network administrator Person responsible for operation, maintenance, and management of a network.

network operator Person who routinely monitors and controls a network, performing such tasks as reviewing and responding to alarms, monitoring throughput, configuring new circuits, and resolving problems.

P

provisioning API A series of BAC functions that programs can use to make the operating system perform various functions.

provisioning groups Groupings of devices with an defined set of associated DPE servers, based on network topology or geography.

R

redundancy In internetworking, the duplication of devices, services, or connections so that, in the event of a failure, the redundant devices, services, or connections can perform the work of those that failed.

regional distribution unit (RDU) Regional Distribution Unit. The RDU is the primary server in the BAC provisioning system. It manages generation of device instructions, processes all API requests, and manages the BAC system.

S

secure sockets layer (SSL) A protocol for transmitting private documents via the Internet. SSL uses a cryptographic system that uses two keys to encrypt data: a public key known to everyone and a private or secret key known only to the recipient of the message. By convention, URLs that require an SSL connection start with *https:* instead of *http:*. BAC 3.0 supports SSLv3.
See TLS

shared secret A character string used to provide secure communication between two servers or devices.

T

template files XML files that contain configuration or firmware rules for devices.

Transport Layer Security (TLS) A protocol that guarantees privacy and data integrity between client/server applications communicating over the Internet. BAC 3.0 supports TLSv1.
See SSL.

TR-069 A standard that defines the CPE WAN Management Protocol (CWMP), which enables communication between CPE and an Auto Configuration Server.

V

Voice over IP (VoIP) A mechanism to make telephone calls and send faxes over IP-based data networks with a suitable quality of service (QoS) and superior cost-benefit.

W

watchdog agent A watchdog agent is a daemon process that is used to monitor, stop, start, and restart BAC component processes, such as the RDU and the SNMP agent.

INDEX

A

C

D

F

L

M

N

P

S

T

U