C H A P T E R **2**

Cisco BAC Architecture

This chapter describes the basic Cisco BAC architecture and includes the following sections:

For more information on each of the components, see the *Cisco Broadband Access Center Administrator's Guide 4.2*.

Regional Distribution Unit

The RDU is the primary server in the Cisco BAC provisioning system. You must install the RDU on a server running the Solaris operating system.

The functions of the RDU include:

- Managing device configuration generation
- Generating configurations for devices and distributing them to DPEs for caching
- Synchronizing with DPEs to keep device configurations up to date
- Processing API requests for all Cisco BAC functions
- Managing the Cisco BAC system

The RDU supports the addition of new technologies and services through an extensible architecture.

Currently, Cisco BAC supports one RDU per installation. To provide failover support, we recommend using clustering software from Veritas or Sun. We also recommend using RAID (Redundant Array of Independent Disks) shared storage in such a setup.

Device Provisioning Engine

The Device Provisioning Engine (DPE) communicates with CPE to perform provisioning and management functions.

The RDU generates DHCP instructions and device configuration files, and distributes them to the relevant DPE servers. The DPE caches these DHCP instructions and device configuration files. The DHCP instructions are then used during interactions with the Network Registrar extensions, and configuration files are delivered to the device via the TFTP service.

Cisco BAC supports multiple DPEs. You can use multiple DPEs to ensure redundancy and scalability.

The DPE handles all configuration requests, including providing configuration files for devices. It is integrated with the Network Registrar DHCP server to control the assignment of IP addresses for each device. Multiple DPEs can communicate with a single DHCP server.

In the DPE, the configurations are compressed using Delta Compression technique to enhance the scalability of the DPE to support up to six million devices.

The DPE manages these activities:

- Synchronizes with the RDU to retrieve the latest configurations for caching.
- Generates last-step device configuration (for instance, DOCSIS timestamps).
- Provides the DHCP server with instructions controlling the DHCP message exchange.
- Delivers configuration files via TFTP.
- Integrates with Network Registrar.
- Provisions voice-technology services.

You must install the DPE on a server that runs the Solaris operating system. Configure and manage the DPE from the CLI, which you can access locally or remotely via Telnet. For specific information on the CLI commands that a DPE supports, see the *Cisco Broadband Access Center DPE CLI Reference 4.2*.

> **Note** During installation, you must configure each DPE for the:
>
> - Name of the provisioning group to which the DPE belongs. This name determines the logical group of devices that the DPE services.
> - IP address and port number of the RDU.

Provisioning Group

A provisioning group is designed to be a logical (typically geographic) grouping of servers that usually consists of one or more DPEs and a failover pair of DHCP servers. Each DPE in a given provisioning group caches identical sets of configurations from the RDU, thus enabling redundancy and load balancing. As the number of devices grows, you can add additional provisioning groups to the deployment.

> **Note** The servers for a provisioning group are not required to reside at a regional location. They can just as easily be deployed in the central network operations center.

Provisioning groups enhance the scalability of the Cisco BAC deployment by making each provisioning group responsible for only a subset of devices. This partitioning of devices can be along regional groupings or any other policy that the service provider defines. To scale a deployment, the service provider can:

- Upgrade existing DPE server hardware
- Add DPE servers to a provisioning group
- Add provisioning groups

To support redundancy and load sharing, each provisioning group can support any number of DPEs. As the requests come in from the DHCP servers, they are distributed between the DPEs in the provisioning group and an affinity is established between the devices and a specific DPE. This affinity is retained as long as the DPE state within the provisioning group remains stable.

Client API

The client API provides total client control over Cisco BAC capabilities. The API enables the client on a remote host to communicate with the RDU.

The API client library exposes the client to a single logical interface. For information on the objects and functions of this interface, see the API Javadocs in the Cisco BAC installation directory. Figure 2-1 shows three remote clients accessing the RDU via the API client library.

Figure 2-1   *Embedded Client Library*
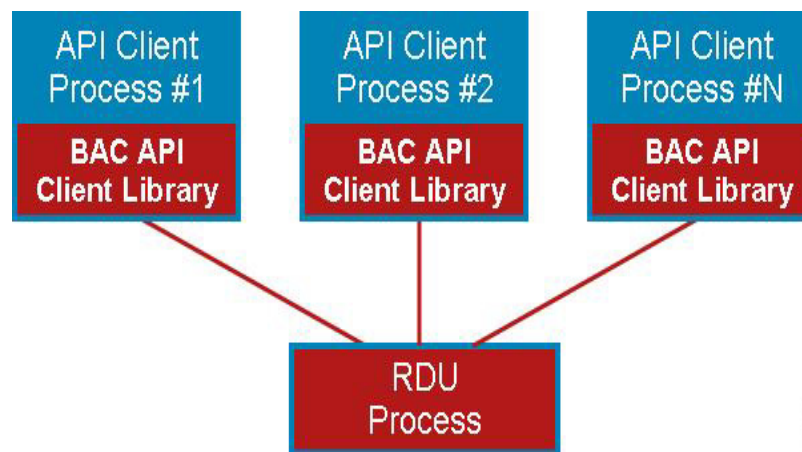
The API client library is packaged in the *bpr.jar* and *bacbase.jar* files, located at *BPR_HOME/lib*, where *BPR_HOME* refers to the home directory on which you install Cisco BAC.

Note   For client communication with the RDU to be successful, ensure that both the *.jar* files are available in the Java classpath and compile against these libraries using the standard Java compilation process.

We recommend that you use Java version 1.6.0_23 or later to support the client API in Cisco BAC.

Cisco Network Registrar

Cisco Network Registrar (CNR) provides the DHCP and DNS functionality in Cisco BAC. The DHCP extension points on CNR integrate Cisco BAC with Network Registrar. Using these extensions, Cisco BAC examines the content of DHCP requests to detect device type, manipulates the content according to its configuration, and delivers customized configurations for devices that it provisions.

For additional information on Network Registrar, see the *User Guide for Cisco Network Registrar 7.2;* *Command Reference Guide for Cisco Network Registrar 7.2*, and *Installation Guide for Cisco Network Registrar, 7.2*.

Key Distribution Center

The Key Distribution Center (KDC) authenticates PacketCable MTAs and also grants service tickets to MTAs. As such, it must check the MTA certificate, and provide its own certificates so that the MTA can authenticate the KDC. It also communicates with the DPE (the provisioning server) to validate that the MTA is provisioned on the network.

The KDC requires a license to function. Obtain a KDC license from your Cisco representative and install it in the correct directory.

For better performance it is recomended to install the KDC on a separate Solaris or Linux server.

The certificates used to authenticate the KDC are not shipped with Cisco BAC. You must obtain the required certificates from Cable Television Laboratories, Inc. (CableLabs), and the content of these certificates must match those that are installed in the MTA.

The KDC has several default properties that are populated during a Cisco BAC installation into the BPR_HOME/kdc/solaris/kdc.ini properties file. You can edit this file to change values as operational requirements dictate.

The KDC also supports the management of multiple realms. For additional details, see *Cisco Broadband Access Center Administrator's Guide 4.2*.

Cisco BAC Process Watchdog

The Cisco BAC process watchdog is an administrative agent that monitors the runtime health of all Cisco BAC processes. This watchdog process ensures that if a process stops unexpectedly, it is automatically restarted. One instance of the Cisco BAC process watchdog runs on every system which runs Cisco BAC components.

You can use the Cisco BAC process watchdog as a command-line tool to start, stop, restart, and determine the status of any monitored processes.

See *Cisco Broadband Access Center Administrator's Guide 4.2* for additional information on how to manage the monitored processes.

SNMP Agent

Cisco BAC provides basic SNMP v2-based monitoring of the RDU and DPE servers. The Cisco BAC SNMP agents support SNMP informs and traps, collectively called notifications.

You can configure the SNMP agent:

- On the RDU, using the SNMP configuration command-line tool or via the API, see the *Cisco Broadband Access Center Administrator's Guide 4.2*.

- On the DPE, using the snmp-server CLI commands, see the *Cisco Broadband Access Center DPE CLI Reference 4.2*.

Table 2-5 in the *Cisco Broadband Access Center Administrator Guide 4.2* lists the Cisco BAC RDU SNMP Traps.

Web User Interface

The Cisco BAC administrator user interface is a web-based application for central management of the Cisco BAC system. You can use this system to:

- Configure global defaults

- Define custom properties

- Add, modify, and delete Class of Service

- Add, modify, and delete DHCP Criteria

- Add, modify, and delete devices

- Group devices

- View server status and server logs

- Manage users