CHAPTER 2

Broadband Access Center Architecture

This chapter describes the system architecture implemented in this Cisco Broadband Access Center (Cisco BAC) release.

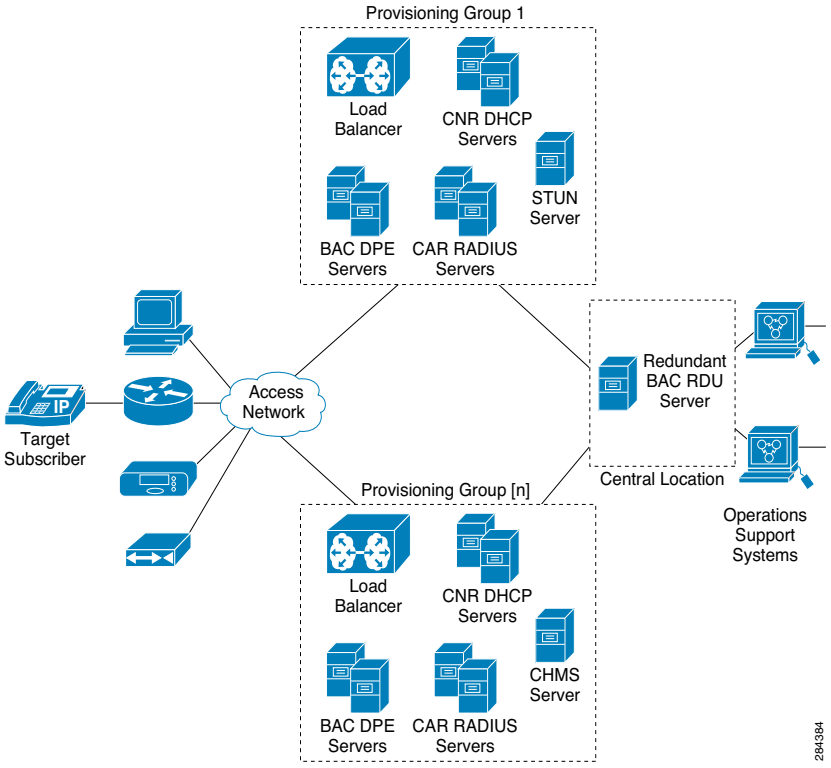
This chapter includes the following sections:

Cisco BAC Deployment

Cisco BAC provisions devices are based on the TR-069, TR-098, TR-104, TR-106, TR-181, and TR-196 standards. This includes Ethernet and ADSL gateway devices, wireless gateways, VoIP ATAs, and other devices compliant with the CPE WAN Management Protocol (CWMP).

Figure 2-1 represents a typical, fully redundant, CWMP deployment in a Cisco BAC network.

Figure 2-1 CWMP Deployment in Cisco BAC



Architecture

This section describes the basic Cisco BAC architecture including:

- Regional Distribution Unit (RDU) that provides:
  - The authoritative data store of the Cisco BAC system.
  - Support for processing application programming interface (API) requests.
  - Monitoring of the system's overall status and health.

  See Regional Distribution Unit, page 2-4, for additional information.
- Device Provisioning Engines (DPEs) that provide:
  - Interface with customer premises equipment (CPE).
  - Configuration and firmware policy instructions cache.
  - Autonomous operation from the RDU and other DPEs.
  - CPE WAN Management Protocol (CWMP) service.
  - IOS-like command line interface (CLI) for configuration.
  - Hypertext Transfer Protocol (HTTP) file service.

  See Device Provisioning Engines, page 2-4, for additional information.

- STUN server:
  - Supports a UDP based connection request mechanism defined in TR069 Annex G to allow Cisco BAC to initiate a session with a CPE that is operating behind a NAT Gateway.
- Cisco Management Heartbeat Server (CMHS) server:
  - A new connection request method that allows Cisco BAC to send connection requests to DLC devices through the CMHS server, using BAC north bound API interfaces or BAC Admin UI.
- Client API that provides total client control over the system's capabilities.
- Provisioning Groups that provide:
  - Logical grouping of DPE servers, CAR-RADIUS servers and CNR-DHCP servers in a redundant cluster.
  - Redundancy and scalability

  See Provisioning Groups, page 2-6, for additional information.
- The Cisco BAC process watchdog that provides:
  - Administrative monitoring of all critical Cisco BAC processes.
  - Automated process restart capability.
  - Ability to start and stop Cisco BAC component processes.
  - Ability to send the SNMP trap if any BAC process fails to start or stop, or stops unexpectedly. SNMP trap is a mechanism that the trap receiver uses to get the information about the process or component failure. A SNMP trap is also sent if Cisco BAC process watchdog fails to start on any of the servers that run Cisco BAC components. Cisco BAC process watchdog reports all the critical conditions of BAC components through SNMP trap.

  See Cisco BAC Process Watchdog, page 2-7, for additional information.

- An administrator user interface that provides:
  - Support for adding, deleting, and modifying CWMP devices; searching for devices, retrieving device details, and running device operations.
  - Support for configuring global defaults and defining custom properties.
  - Ability to view additional performance statistics.
  - Management of firmware rules and configuration templates.

  See Administrator User Interface, page 9-4, for additional information.
- An SNMP agent that supports:
  - Third-party management systems.
  - SNMP version v2.
  - SNMP Notification.

  See SNMP Agent, page 2-7, for additional information.
- Cisco Network Registrar servers that provide:
  - Dynamic Host Configuration Protocol (DHCP).

  See Cisco Network Registrar, page 2-8, for additional information.

Regional Distribution Unit

The Regional Distribution Unit (RDU) is the primary server in the Cisco BAC provisioning system. It is installed on a server running the Solaris 10 or Linux 5.x operating system.

The functions of the RDU include:

- Managing preprovisioned and discovered data from devices.
- Generating instructions for DPEs and distributing them to DPE servers for caching.
- Cooperating with DPEs to keep them 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.

Cisco BAC currently supports one RDU per installation. Use of clustering software from Veritas or Sun is recommended for providing RDU failover. Use of RAID (Redundant Array of Independent Disks) shared storage is recommended in such a setup.

Device Provisioning Engines

The Device Provisioning Engine (DPE) communicates with the CPE on behalf of the RDU to perform provisioning or management functions.

The RDU generates instructions that the DPE must perform on the device. These instructions are distributed to the relevant DPE servers, where they are cached. These instructions are then used during interactions with the CPE to perform tasks, such as configuration of devices, firmware upgrades, and data retrieval.

Each DPE caches information for up to 500,000 devices, and multiple DPEs can be used to ensure redundancy and scalability.

The DPE manages these activities:

- Synchronization with RDU to retrieve the latest set of instructions for caching.
- Communication with CPE using HTTP and HTTPS for file download service.
- Authentication and encryption of communication with CPE.
- Authenticate and Authorize CPE by processing the request from RADIUS server.

The DPE is installed on a server that is running the Solaris 10 or Linux 5.x operating system. The DPE is configured and managed by using the CLI, which you can access locally or remotely using Telnet. See the *Cisco Broadband Access Center 3.8 DPE CLI Reference,* for specific information on the CLI commands that a DPE supports.

See these sections for other important information:

- DPE Licensing, page 2-5
- DPE-RDU Synchronization, page 19-3

Also, familiarize yourself with the concept of instruction generation, which is described in Instruction Generation and Processing, page 4-14.

DPE Extension

The DPE extension interface provides several levels of extensibility that range from ability to make minor changes to existing behavior via an extension to a complete overhaul of DPE behavior that allows it to perform any logic with HTTP or CWMP. It can even function independent of the RDU. The DPE extension simply augments the existing CWMP behavior.

However, when DPE is extended in such a way that RDU is either not required or is not used to store all device records, alternative licensing is needed. The Feature Pack licensing feature, described in DPE Licensing, page 2-5, provides the alternative licenses.

DPE Licensing

Licensing controls the number of DPEs (nodes) that you can use. If you attempt to install more DPEs than you are licensed to have, those new DPEs will not be able to register with the RDU, and will be rejected. Existing licensed DPEs remain online.

Note For licensing purposes, a registered DPE is considered to be one node.

Whenever you change licenses, by adding a license, extending an evaluation license, or through the expiration of an evaluation license, the changes take immediate effect.

When you delete a registered DPE from the RDU database, a license is freed. Since the DPEs automatically register with the RDU, you must take the DPE offline if the intention is to free-up the license. Then, delete the DPE from the RDU database by using the RDU administrator user interface.

Note The functions enabled using a specific license, continue to operate even when the corresponding license is deleted from the system.

Cisco BAC now provides a mechanism to license DPE extension feature packs. The feature pack licenses indicate the count of the devices that can be processed by the feature pack extension. The feature pack licenses can be added to the RDU through Cisco BAC admin UI or API independently with or without CWMP / DPE licenses.

DPEs that are rejected during registration because of licensing constraints, do not appear in the administrator user interface. To determine the license state, you need to examine the log files of the RDU and the DPE.

Provisioning Groups

A provisioning group is designed to be a logical (typically geographic) grouping of servers that usually consist of one or more DPEs, CNR-DHCP servers and CAR-RADIUS servers. Each DPE in a given provisioning group, caches identical sets of instructions from the RDU; thus enabling redundancy and load balancing.

A single provisioning group can handle the provisioning needs of up to 500,000 devices. As the number of devices grows past 500,000, 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.

For more information, see:

- Discovery of ACS URL, page 2-6
- Provisioning Group Scalability, page 2-7

Discovery of ACS URL

In the distributed architecture that Cisco BAC provides, the RDU is the centralized aggregation point that never directly interacts with a CPE. Any required interactions with the CPE are delegated to the provisioning group.

Each device identifies the provisioning group to which it connects by the URL of a single autoconfiguration server (ACS); in other words, the DPE. Until the URL is updated, the device contacts the DPE at the same URL.

All redundant DPEs in a given provisioning group, must share a single ACS URL. The RDU has to be aware of the URL that is associated with each provisioning group and, by extension, of all DPEs in that provisioning group. The RDU uses its knowledge of the provisioning group's ACS URL to redirect devices to a new provisioning group, when required.

The RDU automatically learns the provisioning group's ACS URL from DPE registrations; or the ACS URL is configured on the provisioning group object, using the API or the administrator user interface. For information on configuring the ACS URL, see Provisioning Group Configuration Workflow, page 3-8.

The CPE can determine the ACS (DPE) URL in one of two ways:

- By preconfiguring the URL on the device. This ACS URL is the configured URL of the Cisco BAC server that is associated with each provisioning group. The URL is preconfigured on the device before it is shipped to the customer, and is also known as the assigned URL.

- By discovering the URL via DHCP. This ACS URL is returned in response to a DHCP Discover, a DHCP Request, or a DHCP Inform. This mechanism is limited to deployments of primary Internet gateway devices, because it requires the ability to make DHCP requests to the WAN side.

Note Assigning a URL using preconfiguration is a more secure mechanism than one discovered using DHCP.

Provisioning Group Scalability

Provisioning groups enhance the scalability of the Cisco BAC network 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. When the size of the provisioning group is restricted, the DPEs can be more effective in caching the necessary information.

To scale a deployment, the service provider can:

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

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.

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

See Cisco BAC Process Watchdog, page 9-1, for additional information on how to manage the monitored processes.

SNMP Agent

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

See Monitoring Servers by Using SNMP, page 11-5, for additional information on the SNMP configuration command line tool, and the *Cisco Broadband Access Center 3.8 DPE CLI Reference*, for additional information on the DPE CLI.

Logging

Logging of events is performed at the DPE and the RDU. In some unique situations, DPE events are additionally logged at the RDU to give them higher visibility. Log files are located in their own log directories and can be examined by using any text processor.

You can compress the files for easier e-mailing to the Cisco Technical Assistance Center or system integrators for troubleshooting and fault resolution. You can also access the RDU and the DPE logs from the administrator user interface.

For detailed information on log levels and structures, and how log files are numbered and rotated, see Logging, page 21-2.

Access Registrar

CAR is a RADIUS (Remote Authentication Dial-In User Service) server that enables multiple dial-in Network Access Server (NAS) devices to share a common authentication, authorization, and accounting database.

For additional information on Access Registrar, see the *User Guide for Cisco Access Registrar 5.0* and *Installation Guide for Cisco Access Registrar 5.0*.

RADIUS

CAR is based on a client/server model, which supports AAA (authentication, authorization, and accounting). The client is the Network Access Server (NAS) and the server is CAR. The client passes user information onto the RADIUS server and acts on the response it receives.

The server, on the other hand, is responsible for receiving user access requests, authenticating and authorizing users, and returning all necessary configuration information that the client can then pass on to the user.

Cisco BAC now supports RADIUS for device authentication. CAR provides an extension mechanism to allow customization of RADIUS requests and responses. Cisco BAC handles the Authentication and Authorization request through this extension.

Cisco Network Registrar

Cisco Network Registrar provides the DHCP functionality in Cisco BAC. The DHCP extension points on Network Registrar integrate Cisco BAC with Network Registrar. Using these extensions, the CNR registers itself with Cisco BAC.

Note Cisco Network Registrar (CNR) is re-branded to Cisco Prime Network Registrar starting with the 8.0 release.

For additional information on Cisco Prime Network Registrar, see the *Cisco Prime Network Registrar 8.1 User Guide, Cisco Prime Network Registrar 8.1 CLI Reference Guide*, and *Cisco Prime Network Registrar 8.1 Installation Guide*.

DHCP

The DHCP server automates the process of configuring IP addresses on IP networks. The protocol performs many of the functions that a system administrator carries out when connecting a device to a network. DHCP automatically manages network-policy decisions and eliminates the need for manual configuration. This feature adds flexibility, mobility, and control to networked device configurations.

LeaseQuery

The LeaseQuery feature allows you to request lease information from the Network Registrar DHCP servers. In this release, the LeaseQuery feature is being used by Connection Request and Femto Authorization Service.

The Connection Request performs the LeaseQuery by providing the list of DHCP servers, whereas the Femto Authorization Service performs the LeaseQuery, using the provisioning group. In case of Femto Authorization Service, the DPE sends DHCP LeaseQuery messages only to the DHCP servers registered for the device's provisioning group, which prevents querying all DHCP servers in the network.

Among all responses, the response from the server that last communicated with the devices, is taken as the authoritative answer.

In earlier Cisco BAC versions, the LeaseQuery feature relied on the operating system to select the source interface and the source port for sending LeaseQuery requests. In this release, you can configure the RDU to use a specific interface and source port.

For detailed information on configuring LeaseQuery in this Cisco BAC release, see Configuring Lease Query, page 17-27.