CHAPTER 1

Broadband Access Center Overview

Cisco Broadband Access Center (Cisco BAC) automates the tasks of provisioning and managing customer premises equipment (CPE) in a broadband service provider network.

With the high-performance capabilities of Cisco BAC, you can scale the product to suit networks of virtually any size, even those with millions of CPE. It also offers high availability, made possible by the product's distributed architecture and centralized management.

Cisco BAC supports provisioning and managing of CPE by using the Broadband Forum's CPE WAN Management Protocol (CWMP), a standard defined in the TR-069 specification. Cisco BAC integrates the capabilities defined in TR-069 to increase operator efficiency and reduce network-management problems.

Cisco BAC supports devices based on the TR-069, TR-098, TR-104, and TR-106 standards. These devices include Ethernet and ADSL gateway devices, wireless gateways, VoIP ATAs, and other devices compliant with CWMP. Cisco BAC also provides for runtime-extensible data models to support any upcoming data-model standards or any vendor-specific data models based on CWMP.

Cisco BAC provides such critical features as redundancy and failover. Cisco BAC can be integrated into new or existing environments through the use of a provisioning application programming interface (API) that lets you control how Cisco BAC operates.

You can use the provisioning API to register devices in Cisco BAC, assign device configuration policies, execute any CWMP operations on the CPE, and configure the entire Cisco BAC provisioning system.

Features and Benefits

Cisco BAC helps service providers provision and manage the rapidly expanding number of home networking devices.

Cisco BAC supports mass-scale provisioning and managing of Femtocell Access Point (FAP) devices that function as mini 3G cell tower in customer premises and backhaul call using the customer's internet connection. Apart from supporting the FAP devices, Cisco BAC also supports provisioning and managing of Digital Life Controller (DLC) devices based on TR-069 protocol.

This section describes the basic features and benefits that the Cisco BAC architecture offers:

- Configuration management: Vastly simplified in Cisco BAC through configuration templates, which provide an easy, yet flexible mechanism to assign configurations for CPE. You can use the template-processing mechanism to customize configurations for millions of devices by using a small number of templates.

By using these XML-based templates, you can set configuration parameters and values, and notification and access controls on a device. Configuration templates allow:

  - Conditionals, to include or exclude sections of a template based on, among others, Cisco BAC property values.
  - Includes, to include template content from other files.
  - Parameter substitution, to substitute Cisco BAC property values into template parameters.
  - Prerequisites, to evaluate whether the template is applicable to a device at given time.

- Firmware management: Maintaining and distributing sets of firmware image files to corresponding CPE through the Cisco BAC system. A firmware rules template, associates the firmware image files to groups of devices. Cisco BAC uses the rules in the associated firmware rules template to evaluate the firmware that is downloaded to the device.

  Using the firmware management feature, you can view firmware information on devices, add firmware images to the database, and apply the image files to specific CPE.

- Massive scalability: Enhanced by partitioning CPE into provisioning groups; each provisioning group is responsible for only a subset of the CPE. A provisioning group is designed to be a logical (typically geographic) grouping of servers, usually consisting of one or more Device Provisioning Engines (DPEs).

  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.

- Standards-based security: Cisco BAC is designed to provide a high degree of security by using CWMP, outlined in the TR-069 standard. The CWMP security model is also designed to be scalable. It is intended to allow basic security to accommodate less robust CPE implementations, while allowing greater security for those that can support more advanced security mechanisms.

  Cisco BAC integrates the Secure Sockets Layer (SSL) version 3.0 and the Transport Layer Security (TLS) version 1.0 protocols into its CWMP ACS implementation. By using HTTP over SSL/TLS (also known as HTTPS), Cisco BAC provides confidentiality and data integrity, and allows certificate-based authentication between the various components.

- Easy integration with back-end systems, using Cisco BAC mechanisms such as:
  - The Cisco BAC Java API, which can be used to perform all provisioning and management operations.
  - The Cisco BAC publishing extensions, which are useful in writing RDU data into another database.
  - The Cisco BAC Data Export tool, with which you can write device information from the Cisco BAC system to a file.
  - The SNMP agent, which simplifies integration for monitoring Cisco BAC.
  - The DPE command line interface, which simplifies local configuration when you use it to copy and paste commands.

- Extensive server management: Cisco BAC provides extensive server performance statistics, thereby enabling monitoring and troubleshooting.

- Device diagnostics and troubleshooting: You use this feature to focus on a single device and collect diagnostics information for further analysis. Cisco BAC provides several features to assist diagnosis:
  - Device history—Provides a detailed history of significant events that occur in a device provisioning lifecycle.

- Device faults—Detects devices with recurring faults, which can cause bottlenecks and affect network performance.
- Device troubleshooting—Provides detailed records of device interactions with Cisco BAC servers for a set of devices that are designated for such troubleshooting.
- Direct device operations—Operations such as IP Ping and Get Live Data can be run on the device for more insight.

Supported Technology

This Cisco BAC release supports the provisioning and managing of CPE only through CWMP, outlined in the TR-069 specification. However, virtually any data models based on TR-069, TR-098, TR-104, and TR-106 extensions are supported.

CWMP Technology

TR-069 is a standard for remote management of CPE. This standard defines CWMP, which enables communication between CPE and an autoconfiguration server (ACS).

CWMP details a mechanism that increases operator efficiency and reduces network management problems through its primary capabilities. These capabilities include:

- Autoconfiguration
- Firmware Management
- Status and Performance Monitoring
- Device Diagnostics and Troubleshooting

In addition to CWMP, the TR-069 specification defined a version 1.0 of the data model for Internet Gateway Device (IGD), which has since been expanded by TR-098. CWMP, as defined in TR-069, works with any data model extended from CWMP, including those defined in TR-098, TR-104, and TR-106, upcoming new ones, or those that are vendor specific.