Introduction

This chapter provides an overview of Cisco Broadband Access Center (Cisco BAC), and describes the factors that you must consider before you install Cisco BAC.

Product Overview

Cisco BAC is a distributed and scalable application that automates the tasks of provisioning and managing the Customer Premises Equipment (CPE) in a broadband service provider network. It enables secure provisioning and management of CPE by using the Broadband Forum's CPE WAN Management Protocol (CWMP), a standard defined in the TR-069 specification.

This application is based on open standards and provides a simple and easy way to deploy high-speed data and voice technology.

Cisco BAC can be scaled to suit networks of virtually any size. It also offers high availability, made possible by the product's distributed architecture with centralized management.

Cisco BAC Components

The Cisco BAC component installation program prompts you to install either or all of the following components:

- Regional Distribution Unit (RDU).

  The RDU is the primary server in Cisco BAC provisioning system. You should install the RDU on a Solaris 10 or 11 server, or a Linux 5.x or 6.1 server.

  The RDU:

  - Generates instructions that direct responses from the provisioning group to various customer premises equipment (CPE).
  - Processes application programming interface (API) requests for all Cisco BAC functions.
  - Manages the Cisco BAC system.

  The installation program loads the required data into the RDU database, and starts the RDU daemon through the Cisco BAC watchdog process.

  For details on configuring the SNMP agent, see the *Cisco Broadband Access Center 3.8 DPE CLI Reference*. For information on the Cisco BAC watchdog process, see the *Cisco Broadband Access Center 3.8 Administrator Guide*.

- Device Provisioning Engine (DPE).

  The DPE is the major component of the provisioning group that handles all device interactions with the RDU.

  The DPE:

  - Caches instructions generated at the RDU.
  - Manages the CPE WAN Management Protocol (CWMP) and communicates with the TR-069 enabled devices.

  The installation program installs a CLI on your system to help you to configure the DPE. The Cisco BAC watchdog process and the SNMP agent are also installed for the DPE.

  For information on configuring the DPE and SNMP agent, see the *Cisco Broadband Access Center 3.8 DPE CLI Reference*.

- CNR extensions

  The CNR extensions are the links between Cisco BAC and Cisco Prime Network Registrar. You should install this component on all Cisco Prime Network Registrar servers in your Cisco BAC environment. If you are deploying Cisco BAC in a fail-over environment, ensure that you also install the extensions on the fail-over servers.

  You must install Cisco BAC Cisco Prime Network Registrar extensions on a server running Prime Network Registrar 8.1.3 (and above). If you do not want to install these extensions, you do not need to install Cisco Network Registrar.

- PAR extensions

  The PAR extensions are the links between Cisco BAC and Cisco Prime Access Registrar. You should install this component on all Cisco Prime Access Registrar servers in your Cisco BAC environment. If you are deploying Cisco BAC in a fail-over environment, ensure that you also install the extensions on the fail-over servers.

  You must install the Cisco BAC PAR extensions on a server running Cisco Prime Access Registrar 6.0.1 or later. If you do not want to install these extensions, you do not need to install Cisco Prime Access Registrar.

  Cisco Prime Access Register extensions offers the authentication service for the Femtocell Gateway devices (HNB-GW). This along with the CNR extensions, helps in authentication service.

- STUN server

  Cisco BAC includes a UDP based connection request mechanism defined in TR069 Annex G to initiate a session with a CPE that is operating behind a NAT Gateway. This release of Cisco BAC introduces a STUN service to support the UDP connection request feature.

  STUN service can be run on Solaris or Linux and can be deployed in a different box separately from the RDU and DPE. However, it can be co-located with the DPEs.

  This is an optional component required only when CPE is operating behind a NAT gateway

- SSL Accelerator and Load Balancer.

  SSL Accelerator and Load Balancer manage the traffic from the CPE to DPEs. The SSL accelerator and the Load Balancer enable you to effectively deploy the various hardware devices in the provisioning group.

  We recommend that you use the Cisco ACE 4710 as SSL accelerator and load balancer.