Release Notes for Cisco Broadband Access Center 4.0.1

September 30, 2008

These release notes describe new software features and fixes to software issues in Cisco Broadband Access Center, Release 4.0.1.

Contents

Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Introduction

Cisco Broadband Access Center, referred to as BAC throughout this document, automates the tasks of provisioning and managing customer premises equipment (CPE) in a broadband service-provider network. The application provides a simple and easy way to deploy high-speed data, voice technology, and home networking devices.

BAC can be scaled to suit networks of virtually any size, even those deploying millions of devices. It also offers high availability, made possible by its distributed architecture with centralized management.

BAC incorporates support for many technologies to provide provisioning services for your network. These technologies include:

- DOCSIS high-speed data
- PacketCable voice service, both Secure and Basic workflows
- Non-secure CableHome

System Components

The BAC product comprises:

- The Regional Distribution Unit (RDU), which is the primary server in a BAC deployment. Through its extensible architecture, the RDU supports the addition of new technologies and services.
- The Device Provisioning Engine (DPE), which handles all device interactions with the RDU.
- Cisco Network Registrar extension points, which are the link between BAC and Network Registrar. Network Registrar provides BAC with the DHCP and Domain Name System functionality.
- The Key Distribution Center (KDC), which is a Kerberos server that authenticates PacketCable Multimedia Terminal Adapters (MTAs).
- An administrator user interface, which you can use to monitor and manage BAC.
- A Java provisioning application programming interface (API), which you use to integrate BAC into an existing operations support-system environment.

For information on system requirements, licensing, and upgrading, see Before Installing BAC 4.0.1, page 9. See also the *Installation and Setup Guide for Cisco Broadband Access Center 4.0*.

Supported Devices

BAC provides provisioning and managing of residential devices, namely DOCSIS cable modems and set-top boxes (STBs), PacketCable embedded MTAs (eMTAs), CableHome devices, and computers.

This release of BAC supports provisioning and managing:

- DOCSIS 2.0 IPv4 and IPv6 devices (booted using the IPv4 or IPv6 provisioning flow or dual stack).
- IPv6 devices, including cable modems compliant with DOCSIS 3.0, computers, and set-top boxes (STBs).

- Video STBs, specifically the RNG-200 STB for IPv4 and IPv6 that is based on the evolving OpenCable Application Platform.
- Variants of eSAFE (embedded Service/Application Functional Entities) devices, such as mixed-IP mode PacketCable MTAs. A mixed-IP mode MTA is an eSAFE device that consists of an IPv6 embedded cable modem and an IPv4 eMTA. This class of devices embeds additional functionality with cable modems, such as packet-telephony, home networking, and video.

As in previous releases, BAC continues to provision:

- Cable modems and STBs compliant with DOCSIS 1.0, 1.1, and 2.0.
- eMTAs compliant with PacketCable version 1.5
- Devices compliant with CableHome 1.0.
- Computers.

Supported Standards

BAC complies with these applicable Requests for Comments (RFCs), protocols, standards, and Internet Engineering Task Force (IETF) drafts:

- IPv6—Complies with RFC 2460 (IPv6 specification), 2461 (Neighbor Discovery protocol), 2462 (Stateless Address Autoconfiguration), 2463 (Internet Control Message Protocol–ICMP), 3513 (Addressing Architecture).
- DHCPv6—Complies with RFC 3315 (DHCPv6 specification), 3633 (IPv6 Prefix Options), 3736 (Stateless DHCP Service for IPv6), 4014 (Remote Authentication Dial-In User Service–RADIUS–Attributes Suboption for the Relay Agent Information Option), 4580 (Relay Agent Subscriber-ID Option), 4649 (Relay Agent Remote-ID Option), and 4704 DHCPv6 Client Fully Qualified Domain Name (FQDN) Option.
- IPv4 and IPv6 interoperability—Complies with RFC 4038 (Application of IPv6 Transition) and 4472 (Operational Issues and Considerations with IPv6 DNS).
- TFTP and ToD servers—Complies with RFC 868 (Time Protocol) and 2349 (TFTP Blocksize Option).

Additionally, BAC complies with these applicable CableLabs and Comcast standards:

- DOCSIS 3.0 Specifications:
  - CM-SP-SECv3.0-I04-070518
  - CM-SP-PHY3.0-I04-070518
  - CM-SP-MULPIv3.0-I04-070518
  - CM-SP-OSSIv3.0-I03-070518
- DOCSIS 2.0 Specifications:
  - CM-SP-RFI2.0-I12-071206
  - CM-TR-DOCSIS2.0-IPv6-V01-080307
- DOCSIS L2VPN Specification CM-SP-L2VPN-I06-071206
- PacketCable MTA Device Provisioning Specification PKT-SP-PROV1.5-I03-070412
- CableHome CH-SP-CH1.0-I05-030801

- COMCAST-SP-RNG-200-ProvOSS-I04-070102
- OpenCable specification OC-SP-HOST2.0-CFR-I13-070323

New and Changed Features

These sections briefly describe enhancements in the 4.0.1 release and new or modified features in the 4.0 release that also apply to the 4.0.1 release:

Enhancements in BAC 4.0.1

BAC 4.0.1 includes the following enhancements in addition to those that apply to BAC 4.0:

- Support for DOCSIS 2.0 + IPv6 devices.
- Support for RNG-200 devices for IPv4 and IPv6, including dual-stack RNG-220s.
- Support for a newer Java version (JRE 1.6.0_04). Earlier versions are no longer supported, except for a BAC API client operating with the BAC 4.0.1 RDU. See System Requirements, page 9.
- Direct or incremental upgrades from these BAC versions:
  - 2.7.1.*x*.
  - 2.6.2.*x* that BAC 4.0 already supports.
  - 4.0—Customers using the BAC 4.0 RDU must first upgrade to 4.0.0.1.

  See Upgrading to BAC 4.0.1, page 12.
- Processing of DHCP Option 177 Requests. See Additional Notes for BAC 4.0.1, page 8.
- Provisioning of Promiscuous Mode MTA Devices. See Additional Notes for BAC 4.0.1, page 8.

DOCSIS 3.0 and IPv6 Support

This BAC release introduces support for DOCSIS 3.0, which defines the third generation of the high-speed data-over-cable systems specification. DOCSIS 3.0 provides:

- Provisioning of IPv6 devices
- Expanded addressability of network elements

- Increased channel capacity via channel bonding
- Enhanced network security
- Enhanced multicast capabilities
- New service offerings

This release enhances these existing features in BAC to facilitate IPv6 transport:

- **Lease Query**—You can request current IP address information directly from the Network Registrar DHCP servers in a provisioning group. This feature, thus, provides:
  - IP address information for device resets and management.
  - Reporting details of IPv4 and IPv6 devices.

  You can also configure the IP addresses of the DHCP servers in the provisioning group using an autoconfiguration mechanism, which makes for easier network administration.
- **TFTP service**—The DPE's high-performance TFTP service allows on-delivery customization that DOCSIS uses to mix time-sensitive information into the file that is to be delivered. This BAC release enhances the TFTP service to:
  - Support IPv6 transport.
  - Support compression of dynamic TFTP files that a DPE caches, thus enhancing DPE performance.
  - Provide an optional block-size option, which specifies the number of data octets and allows the client and server to negotiate a block size more applicable to the network medium. The block-size option in BAC complies with RFC 2348.
  - Maintain statistics for the number of TFTP packets that are processed for TFTPv4 and TFTPv6.
- **ToD (Time of Day) service**—The DPE's ToD service provides high-performance UDP implementation of RFC 868. This service provides:
  - Support for IPv6 transport.
  - Statistics for the number of ToD packets that are processed for ToDv4 and ToDv6.
- **SNMP support**—The BAC RDU supports SNMP management over IPv6 to provide device disruption for IPv6 cable modems and STBs.

STB Support

This BAC release introduces support for the video STB, specifically the RNG-200 STB, which is based on the evolving OpenCable Application Platform.

Enhanced Scalability and Performance

This BAC release provides:

- Massive scalability of the RDU and the DPEs in your network. The RDU can support up to 60 million devices, and a provisioning group can support 2 million devices, of which 500,000 can be Secure PacketCable devices.
- Enhanced DPE synchronization with the RDU, rendering the process in the background so that the RDU is not overloaded with synchronization requests. The process is also updated to support requests for the DPE based on the DHCP Unique Identifier (DUID) of an IPv6 device.

- Enhanced performance of the template parser (which DOCSIS, PacketCable, and CableHome extensions use to provide dynamic configurations) to optimize generation of device configurations based on templates. Additionally, you can compress all configurations that are generated, thus decreasing overhead at the DPE to enhance server performance.
- Enhanced multivendor support by enabling scoping of Option 43 and its suboptions. It also gives you the option of using a single template to specify various TLV 43s from many vendors.

Improved Management

This BAC release enables you to manage your network better by introducing support for:

- Provisioning group properties on the property hierarchy—Enhances the flexibility that the BAC property hierarchy provides by including the properties of a device's provisioning group.
- Provisioning group capabilities—Allows you to control the device type support that must be enabled for the provisioning groups in your deployment. In earlier BAC releases, each DPE in a provisioning group registered what it was capable of supporting with the RDU at startup. This information was combined with that of other DPEs in the provisioning group to determine the device types that the group could support. Thus, the capabilities of a provisioning group were automatically enabled.

  In this release, however, you must manually enable the capabilities of a provisioning group from the administrator user interface or the API. You can thus choose to enable only specific capabilities and ignore others in keeping with your requirements.
- "Services" interface on the DPE command line—Provides flexibility in configuring the DPE to suit your requirements. Using the "services" interface, you can choose to enable only certain services; for example, you can enable the TFTP service for IPv4 transport, but not for IPv6 transport. All services on the DPE are by default disabled.

Increased Security

This BAC release provides increased security via:

- User-configurable IP addresses and ports to support:
  - **Multipathing**—Earlier BAC versions enable you to configure a DPE interface for provisioning using the Solaris interface names. This BAC release enables you to configure the provisioning interfaces using the IP addresses of the DPE interface, thus allowing one interface to back up for another by switching its IP address in case of failure.
  - **Multi-interface binding**—When communicating with Network Registrar extension points, previous BAC DPEs rely on the operating system to determine the interface for use, because the extensions require the reply to come from the interface that the request was sent to. In this BAC release, you can configure this interface, which by default is all IPv4 interfaces.
  - **Firewall compatibility**—Earlier BAC releases rely on the operating system to determine the source interface and the source port in communications between the DPE and the RDU. In this BAC release, you can configure the source interface and the port, and thus segment management traffic and create firewall rules.
- **CMTS MIC for DOCSIS 3.0**—Supports DOCSIS 3.0 for the Extended CMTS MIC Configuration Setting that configures how the CMTS checks the integrity of a message. By providing 3.0 support for this setting, BAC uses advanced hashing techniques to detect unauthorized modification or corruption of the cable modem configuration file.

- **Password policy**—Enforces a password policy to access the RDU from the administrator user interface. The password that you use to log in to the administrator user interface must have at least 8 characters.
- **HTTP over SSL (HTTPS)**—Provides access to the administrator user interface using a secure SSL connection.

Enhanced Troubleshooting and Diagnostics

This BAC release provides options for:

- **Device troubleshooting using the device ID**—Enhances device troubleshooting to provide detailed records of device interactions with BAC servers using the IDs of the devices designated for troubleshooting. Using this feature, you can focus on a single device, identified by its MAC address or its DUID, and use that diagnostic information for further analysis.
- **Server troubleshooting using diagnostics tool**—Provides diagnostics scripts to collect performance statistics, down to a specific type of statistic, for BAC servers. Using individual scripts, you can:
  - Gather diagnostics concurrently.
  - Determine the status of diagnostics collection.
  - Stop diagnostics prematurely.

  This release also provides many scripts to collect server and system configuration data that may be required for support escalations. You can use additional scripts to bundle the diagnostics data for support.

New Installation

This BAC release provides an improved and flexible installer that uses the Solaris package system, rather than the InstallShield installer. The package installer gives you the option of installing from the command-line interface in interactive or noninteractive modes.

Automated Migration

This BAC release supports:

- Automatic migration of the RDU database from the 2.7.1.*x* and 2.6.2.*x* versions to 4.0.1.
- Automatic migration of the DPE cache.
- Compatibility of the 4.0.1 RDU and DPE with earlier versions of Solaris DPEs and Network Registrar servers, respectively, for gradual online migration.

Licensing Using Cisco Standard

This BAC release enhances licensing to provide flexible options, greater reliability and security, and ease of use. While earlier BAC versions used a proprietary model of licensing, this release incorporates support for FlexLM, a Cisco license management system.

In previous BAC releases, you were licensed for the technologies that provisioned the devices in your network. In this release, you are licensed to provision a specific number of services for any device type. Each service translates to three IP addresses that are provisioned in the system.

See also Licensing, page 10.

Additional Notes for BAC 4.0.1

The following changes also apply to BAC 4.0.1:

Processing DHCP Option 177 Requests

BAC now properly handles incoming requests from legacy devices that support DHCP option 177, which was deprecated and replaced by option 122 (cable-labs-client-configuration; see http://www.cisco.com/en/US/docs/net_mgmt/broadband_access_center_for_cable/4.0/administration/guide/app_C.html).

A BAC 4.0 DHCP extension that received a PacketCable eMTA DHCPDISCOVER packet containing option 177 would drop the packet. The workaround was not to install BAC 4.0 in deployments of legacy MTAs supporting DHCP option 177 (CSCso61910). BAC 4.0.1 now correctly provisions legacy devices that use Option 177.

Provisioning Promiscuous Mode MTA Devices

A promiscuous MTA device is allowed to boot and be configured without being preregistered in BAC and whose provisioning is based on policies assigned to its relay agent.

Promiscuous mode is allowed in BASIC.1and BASIC.2 workflows only; it is not applicable to SECURE workflows. See:

- http://www.cisco.com/en/US/docs/net_mgmt/broadband_access_center_for_cable/4.0/administration/guide/chap_4.html#promiscuous_access_for_devices
- http://www.cisco.com/en/US/docs/net_mgmt/broadband_access_center_for_cable/4.0/administration/guide/chap_7.html).

In BAC 4.0, MTA devices did not provision correctly in the promiscuous mode, even with the PacketCable Promiscuous Mode enabled and the PacketCable Promiscuous Class of Service set at the system level (CSCsq40930). The DOCSIS configuration would be correct, but the DHCPOFFER sent to the MTA would be missing the fully qualified domain name (FQDN), hence the MTA could not be provisioned.

The workaround would be to configure a client-class in Network Registrar first:

1. Log in to the Network Registrar web UI.
2. Be sure that there is a policy and scope to handle unprovisioned devices. If not, go to the Add DHCP Policy page to add a policy for those devices, then to the Add DHCP Scope page to add a scope that points to that policy.
3. Define a client-class that points to the policy. On the Add (or Edit) DHCP Client-Class page, enter **@use-macaddress** for the hostname, which synthesizes a hostname based on the MAC address of the device, then enter the domain name. Save the client-class and reload the DHCP server.
4. Exit Network Registrar and log in to the BAC administrator user interface.

5. On the Configure Defaults > System Defaults page, under Promiscuous Policy Settings, ensure that the PacketCable Promiscuous Mode is set to Enabled. The PacketCable Promiscuous DHCP Criteria and PacketCable Promiscuous Class of Service should also be set to the name of the Network Registrar DHCP client-class that handles unprovisioned MTAs.
6. Submit the changes.

Promiscuous Mode Disabled After Migration

When migrating to BAC 4.0.1 from 2.6.2.*x*, a PacketCable MTA's promiscuous access is disabled after the migration, though promiscuous mode is enabled in 2.6.2.*x* (CSCsr65051). This behavior, however, is expected because in 2.6.*x*, the property */modem/promiscuousMode* is only relevant to non-PacketCable technologies.

When migrating to BAC 4.0.1 from 2.7.1.*x* versions, if promiscuous mode is enabled in 2.7.*x*, it is retained. This behavior is also expected because the */modem/promiscuousMode* property in 2.7.*x* applies to all technologies, including PacketCable.

Before Installing BAC 4.0.1

Review the following information before you begin to install BAC 4.0.1.

System Requirements

To successfully install BAC 4.0.1 on your system, you must meet these requirements:

- **Operating system**—You must install BAC on a Sun SPARC platform running the Solaris 9 or 10 operating system with at least 4 GB of memory. Cisco recommends that you use a Sun SPARC multiprocessor platform.

  Note When enabling IPv6 support, you must use the Solaris 10 operating system.

- **Network Registrar**—You must have Cisco Network Registrar version 7.0 installed on the servers on which you are installing BAC extensions.
- **Administrator user interface**—At a minimum, you must have Microsoft Internet Explorer 6.0 (Service Pack 2) or Firefox 1.5.
- **API client**—Ensure that:
  - You install Java 1.6.0_02 to support the API client in release 4.0. API clients in versions earlier than 4.0, however, support JRE versions earlier than 1.6_0_02.
  - The files *bpr.jar* and *bacbase.jar* are available in the classpath.

Licensing

This BAC release moves away from the proprietary licensing model used previously and incorporates support for the FlexLM licensing system, a Cisco license management system. The new system provides enhanced reliability and security, ease of use, and flexible licensing options.

Obtaining the Licenses

Each license in this release is available as a permanent license or an evaluation license.

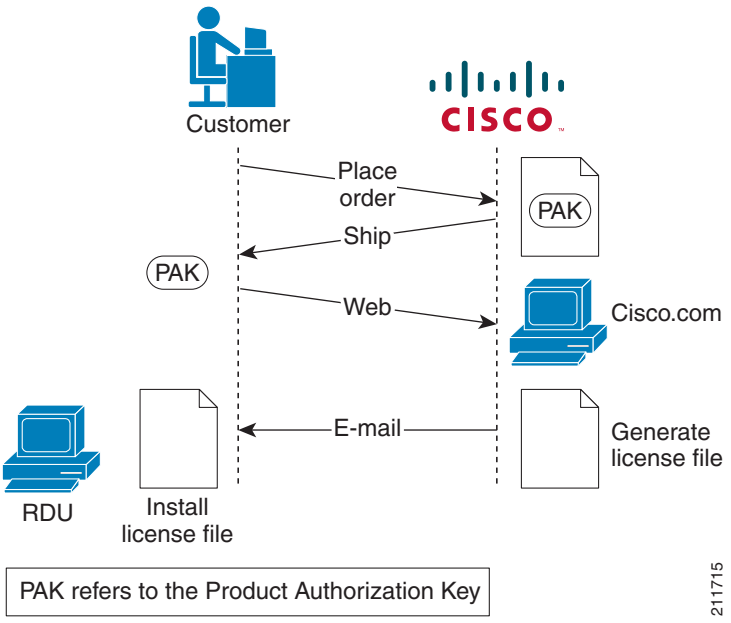
- **Permanent**—You purchase a permanent license for use in your network environment and to activate the specific features for which it is intended.
- **Evaluation**—You purchase an evaluation license to enable functionality for a specific length of time. You can upgrade an evaluation license to a permanent license.

Caution Do not attempt to deploy into a fully operational network with an evaluation license. When the evaluation license expires, you will not be able to use BAC to provision the devices in your network.

Obtaining a Permanent License

To request a permanent license, follow the procedure that Figure 1 depicts.

Figure 1 License Claim Process



Note With FlexLM licensing, you receive a Product Authorization Key (PAK) for each software CD package that you purchase. The PAK is affixed as a sticky label on the Software License Claim Certificate card that is included in your CD-ROM package.

To obtain a permanent license:

1. Keep your PAK handy and access http://www.cisco.com/go/license. You must have a valid Cisco.com account to log in to this site.

   The Product License Registration website appears.

2. Complete the steps detailed at the Product License Registration page.

   Note During license registration, submit each PAK that you have received. For each PAK that you submit, a license file is generated and sent to you via e-mail.

3. Once you receive your license file, install it using the procedure described in Installing the License, page 11.

Obtaining an Evaluation License

For an evaluation license, contact your Cisco representative, who will generate the necessary key from the Cisco licensing website and e-mail it to you. Once you receive your license file, install it using the procedure described in Installing the License, page 11.

Installing the License

Before installing the license file, ensure that you back up your licenses in case you have to reinstall the BAC software.

To install a permanent or evaluation license:

Step 1 Once you receive your license file, save each file to the system on which you plan to launch the BAC administrator user interface.

Step 2 Launch your web browser on that system.

Step 3 Enter the administrator's location using this syntax:

```
http://machine_name:port_number/
```

Note To access the administrator user interface via HTTPS, enter:

```
https://machine_name:port_number/
```

- *machine_name*—The machine on which the RDU is running.
- *port_number*—Port on which the server side of the administrator application runs. The default port is:
  - 8100 for HTTP over TCP
  - 8443 for HTTP over SSL

The main login page appears.

Step 4 Enter the default username (**admin**) and the default password (**changeme**).

a. If you are logging in for the first time, the Change Password screen appears.

b. Enter a new password and confirm it. Ensure that the password that you enter has at least 8 characters.

Step 5 Click **Login**.

The Main Menu page appears.

Step 6 Click the license link at the top of the Main Menu page, or choose **Configuration > License Keys**.

The Manage License Keys page appears.

Step 7 In the License File field, enter the complete path to the location of the license file on your local system. Remember to include the name of the license file while specifying the pathname. Or, click **Browse** and navigate to the license file.

Step 8 Click **Add/Upgrade**.

The details regarding the number of services and the DPEs that you are licensed to use appear.

Installation Notes

Review the following notes before installing BAC 4.0.1.

- Ensure that your system meets the requirements described in System Requirements, page 9.
- Ensure that you download and install the recommended patches from the Sun Microsystems support site.
- Obtain the BAC license file, as described in Obtaining the Licenses, page 10. Then install the license, as described in Installing the License, page 11.
- Verify the file-system block size of the directory in which you intend to install the BAC database and database transaction log files. For optimum performance and reliability of the BAC database, configure the file system or systems that contain the database files and database log files with an 8-KB or greater block size.
- Ensure that the file system in which you place database files is configured to support files larger than 2 GB.

For complete information on installation procedures, refer to the *Installation and Setup Guide for Cisco Broadband Access Center 4.0*.

Upgrading to BAC 4.0.1

BAC 4.0.1 provides upgrades from:

- 2.7.1.*x*.
- 2.6.2.*x* that BAC 4.0 already supports.
- 4.0—Customers using the BAC 4.0 RDU must first upgrade to 4.0.0.1.

See Table 1.

Upgrade the BAC components in this order:

1. Upgrade the RDU and client APIs simultaneously.
2. In each provisioning group, upgrade the DPEs first, followed by the KDC, then the Network Registrar extensions.

Note BAC 4.0.1 features are available only after the administrator explicitly enables them. You cannot upgrade DPE appliances; only Solaris DPEs are supported.

Upgrade Tasks

The upgrade tasks described in Table 5-1 in Chapter 5 ("Upgrading Broadband Access Center") of the *Installation and Setup Guide for Cisco Broadband Access Center 4.0* should be amended as in Table 1.

Table 1 Upgrading to BAC 4.0.1

Version	RDU	DPE	KDC	Network Registrar Extension Points
BAC 2.7.1.*x* **Note** Migration of RDU database is required.	Run **pkgadd**. At the end, the installer prompts you to run the migration tool. (See Migration Tool, page 13.)	Run **pkgadd** to upgrade the DPE.	Run **pkgadd** to upgrade the KDC.	Run **pkgadd** to upgrade the Network Registrar extensions.
BACC 2.6.2.*x* **Note** Migration of RDU database is required.				
BAC 4.0 **Note** Migration of RDU database is not required.	1. Upgrade to BAC 4.0.0.1 2. Run **pkgadd**. You do not need to run the migration tool.	Run **pkgadd** to upgrade the DPE.	Run **pkgadd** to upgrade the KDC.	Run **pkgadd** to upgrade the Network Registrar extensions.

When upgrading to 4.0.1, you must enter a new target location for these directories:

- Home (*BPR_HOME*)—This prompt is the only one in a 4.0.0.1-to-4.0.1 migration.
- Data (*BPR_DATA*)
- Database logs (*BPR_DBLOG*)

Migration Tool

In Table 5-3 in Chapter 5 ("Upgrading Broadband Access Center") of the *Installation and Setup Guide for Cisco Broadband Access Center 4.0*, the **–cmtsv** flag is used only in migrating from 2.6.*x* and later releases to 4.0 and 4.0.1. The flag is not used in migrating from 2.7.1.*x* or later, which uses an internal property setting.

For 4.0.1, the default **–cmtsv** value was changed from 1.1 to 1.0.

4.0.1 also includes changes to the default values to certain promiscuous device settings for the **migrateDb.sh** tool (see Table 2).

Table 2 Promiscuous Device Settings for migrateDb.sh Tool

Argument	Description	Required	Optional	Default
-pdcpc *value*	Specifies the name of the most frequently used DHCP Criteria for promiscuous computers		✓	unprovisioned-computer
-pdcmta *value*	Specifies the name of the most frequently used DHCP Criteria for promiscuous MTAs		✓	packet-cable-mta
-pdcchwd *value*	Specifies the name of the most frequently used DHCP Criteria for promiscuous CableHome WAN-Data devices		✓	unprovisioned-cablehome wan-data
-pdcchwm *value*	Specifies the name of the most frequently used DHCP Criteria for promiscuous CableHome WAN-MAN devices		✓	unprovisioned-cablehome wan-man
-pdccpe *value*	Specifies the name of the most frequently used DHCP Criteria for promiscuous custom CPE		✓	unprovisioned-customcpe

System Hardening

This BAC release has undergone comprehensive security testing. The objective of this security testing was to identify and eliminate any security vulnerabilities pertaining to BAC and its supporting software and hardware. This release was also tested for protocol robustness, which tests for application stamina when exposed to Denial of Service attacks and protocol irregularities.

For this release, the security testing was performed using *5.10 Generic_127127-11 sun4v sparc SUNW, Solaris 10 5/08 s10s_u5wos_10*, hardened with Solaris Security Toolkit 4.2.

To mitigate security threats when deploying a BAC release, Cisco recommends that you harden the systems.

Note Complying to these recommended hardening guidelines does not guarantee the elimination of all security threats. However, implementing these recommended guidelines will achieve a higher level of security and help manage unforeseen risk.

We recommend that you complete the following activities to harden your systems:

- Ensure that all Sun Microsystems-recommended OS and Security patches have been applied. Contact Sun Microsystems Support to download the recommended patches and check for any applicable updates.
- Disable all unused network services. At a minimum, run the following Solaris command:

  ```
  # netservices limited
  ```

- Use the latest version of the Solaris Security Toolkit to assist with system hardening.

- Disable unused daemons and services, especially services that use network resources; for example:

```
# svcadm disable svc:/network/smtp:sendmail
# svcadm disable svc:/network/finger:default
```

- Uninstall all unused applications.
- Apply the highest level of password protection to all network applications and services. Ensure that you change the default passwords.
- Use HTTPS to access the BAC administrator user interface and disable the HTTP access. HTTP access to the administrator user interface (using port 8100) is enabled by default on the RDU. Currently, there is no way to disable the HTTP service using standard BAC administrative methods. You can, however, disable HTTP access using the Tomcat server.xml file, which is located at *BPR_HOME*/rdu/tomcat/conf.

  To do this:

  a. Comment out the HTTP/8100 connector directive in the Tomcat server.xml file. For example:

```
<!-- <Connector port="8100" maxHttpHeaderSize="8192"
maxThreads="150" minSpareThreads="25" maxSpareThreads="75"
enableLookups="false" redirectPort="9453" acceptCount="100"
connectionTimeout="20000" disableUploadTimeout="true" /> -->
```

  b. Reload the Tomcat process to make your changes take effect. For example:

```
# /etc/init.d/bprAgent restart tomcat
Process [tomcat] has been restarted.
```

- If SNMP is not being used to manage the BAC components, then shut down the SNMP service. The SNMP service is enabled by default on the RDU and DPEs. This SNMP service uses UDP port 8001. You can disable this service for the RDU or a DPE using the **snmpAgentCfgUtil.sh stop** command from *BPR_HOME*/snmp/bin. For example:

```
# ./snmpAgentCfgUtil.sh stop
Process [snmpAgent] has stopped.
```

Caveats

For information on the complete list of BAC bugs, see the BAC401_BugList.html file in the /docs subdirectory of the BAC CD-ROM, or at the BAC software download site on http://www.cisco.com.

Fixed Bugs in BAC 4.0.1

Table 3 lists major software issues fixed in BAC 4.0.1.

Table 3 Bugs Fixed in BAC 4.0.1

CDETS Number	Description
CSCeg87139	The TFTP server suffers from Sorcerer's Apprentice Syndrome. When the server receives a bad ACK for a previous data block but not for the one that was sent out last, it automatically resends the data block instead of waiting for the real ACK.

Table 3 Bugs Fixed in BAC 4.0.1 (continued)

CDETS Number	Description
CSCeh19809	An external file associated with the property */docsis/cmts/version/giaddrToVersionMap* can be deleted even if it is being used in DOCSIS defaults, resulting in configuration generation failures for DOCSIS devices.
CSCse51856	The DPE crashes with an out-of-memory error when the TFTP server handles files larger than 20 MB.
CSCsl39607	During installation, the program does not check for sufficient disk space to accommodate BAC log files, which can take up to 25 MB per log.
CSCsl71128	When upgrading the DPE from 2.6.*x* to 4.0, the dpe.properties file does not upgrade properly.
CSCsl87226 CSCso69297	After an upgrade from 2.6.2.*x*, the Network Registrar extension points fail to register with the RDU. This error occurs when you upgrade Network Registrar extensions that were previously enabled for PacketCable.
CSCsm12796	If the RDU batch queues are full, BAC may drop a batch posted by a DPE server, in which case the RDU sends a dropped batch status back to the client. When the DPE receives the status, it immediately posts another batch, forcing the RDU to drop batches at a high rate when the RDU is already overloaded.
CSCsm12864	When a batch posted by the DPE server is dropped by the RDU, the DPE may immediately post a batch to the RDU containing a remote logging command to log a record of the DPE problem in the RDU log. Since the RDU dropped the DPE batch because it was overloaded immediately posting another batch likely causes the RDU to spend time dropping another batch instead of working on the batches already queued.
CSCsm15697	After a DPE upgrade from 2.6.2.7 on Solaris 9, if the time server is already running, the upgrade does not stop the process. When the DPE starts after the upgrade is complete, it stops because of a bindException.
CSCsm37705	When running **captureConfiguration.sh** on a server on which the DPE, Network Registrar extensions, or KDC components are installed, the script does not capture any configuration or log files for the BAC component.
CSCsm59972	The response time of the RDU API IPDevice.getDetails() command degrades steadily over time under stress load.
CSCsm72069 customer case	When upgrading firmware for a CableLabs device, it may report different or additional DHCP option 60 modem capabilities. Consequently, the option is not fully validated, resulting in the RDU never receiving the updated value.

Open Bugs in BAC 4.0.1

Table 4 lists major software issues open in BAC 4.0.1.

Table 4 Bugs Open in BAC 4.0.1

CDETS Number	Description	Workaround/Resolution
CSCsl17155	The DPE View Log File icon does not function in DPEs in BAC versions earlier than 2.7.	View the logs by using the CLI on the DPE.
CSCsm43002	The **captureConfiguration.sh** script copies the agent log files, but not the agent/conf/* files (agent.conf).	Copy the agent/conf/* files manually.
CSCso85401	The cable modem rejects the config file because of an incorrect DOCSIS shared secret. The DOCSIS shared secret value is set in the *dpe.properties* and *local.properties* files. If you deleted the DOCSIS shared secret from the DPE command line using the **no docsis shared-secret** command, the DOCSIS shared secret is removed from dpe.properties but remains in the local.properties file.	Reload the DPE to remove the DOCSIS shared secret from local.properties.
CSCsr70925	An upgrade fails after you receive the following message: `Port 8100 in use/Installer abort with 8100 port in use`	This error occurs if the upgrade script does not stop the bprAgent service. The workaround is to: 1. Stop the bprAgent from the command line using: `# /etc/init.d/bprAgent stop` 2. Resume the upgrade.
CSCsu50653	The RDU database fails to start on a ZFS, with an *`InitializedFailException`* error appearing after a reboot.	BAC does not support the ZFS and therefore, you must not use a ZFS for the RDU database.
CSCsu54215	During installation, the installer does not display an error message when the /tmp folder is full.	Before you run the installer, ensure that you have at least 500 MB of free disk space for the /tmp folder.

Documentation Errata

The following errata exist in the documentation for BAC 4.0:

- *Cisco Broadband Access Center DPE CLI Reference*—Chapter 3, “DPE Configuration Commands” (see http://www.cisco.com/en/US/docs/net_mgmt/broadband_access_center_for_cable/4.0/command/reference/Ch_3.html):
  - For the **interface ip provisioning** command on page 3-13, in the “Syntax Description,” the first numbered item on deleting an existing IP address should have the command syntax **no interface ip** *ip_address* **provisioning**, with the IP address included. (CSCsq61680)
  - For the **service tftp ipv4 | ipv6 blocksize** command on page 3-17, in the “Defaults” section of Table 3-2, the default upper and lower limits for IPv4 block sizes should be 512 and 1428 bytes, respectively. The IPv6 block sizes should both be 1448 bytes. (CSCsm67127)
  - For the **service tftp ipv4 | ipv6 enabled** command on page 3-18, the well-known TFTP port is 69, not 60 as indicated. (CSCsq61680)
- *Installation and Setup Guide for the Cisco Broadband Access Center*—Chapter 5, “Upgrading Network Registrar Extensions” (see http://cisco.com/en/US/docs/net_mgmt/broadband_access_center_for_cable/4.0/installation/guide/Chap5.html):
  - On page 5-4, in “Upgrading Network Registrar Extensions,” the 4.0 extension points must be properly activated following an upgrade. To do this, the following step has been added to the procedure:

    Step 6 Enable the Network Registrar extensions by running the following **nrcmd** command from the Network Registrar home directory (being sure to include the redirect to the file).

    For example:

    ```
    # /opt/nwreg2/local/usrbin/nrcmd -s -b
    < /opt/CSCObac/cnr_ep/bin/bpr_cnr_enable_extpts.nrcmd
    ```

    (CSCso78513)
- *Installation and Setup Guide for the Cisco Broadband Access Center*—Chapter 3, "Installing Broadband Access Center" (see http://www.cisco.com/en/US/docs/net_mgmt/broadband_access_center_for_cable/4.0/installation/guide/Chap3.html):
  - On page 3-3, in "Installing BAC," unpacking the file with the .gtar extension. To do this, the following step has been changed to the procedure:

    Step 2 c. Unpack the file with the .gtar extension that gunzip decompressed. Enter:

    ```
    gtar -xvf BAC_400_SolarisK9.gtar
    ```

    (CSCsr53611)

Related Documentation

These related guides support this BAC release:

- *Installation and Setup Guide for Cisco Broadband Access Center 4.0* (http://www.cisco.com/en/US/docs/net_mgmt/broadband_access_center_for_cable/4.0/installation/guide/InstallGuide40.html)

- *Cisco Broadband Access Center DPE CLI Reference 4.0* (http://www.cisco.com/en/US/docs/net_mgmt/broadband_access_center_for_cable/4.0/command/reference/DPECLIRef40.html)
- *Administrator Guide for Cisco Broadband Access Center 4.0* (http://www.cisco.com/en/US/docs/net_mgmt/broadband_access_center_for_cable/4.0/administration/guide/AdminGuide40.html)

Additionally, you can refer to:

- *Release Notes for Cisco Network Registrar 7.0* (http://cisco.com/en/US/docs/net_mgmt/network_registrar/7.0/release/notes/CNR70ReleaseNotes.html)
- *Installation Guide for Cisco Network Registrar 7.0* (http://cisco.com/en/US/docs/net_mgmt/network_registrar/7.0/installation/guide/CNR70Install_Book.html)
- *User Guide for Cisco Network Registrar 7.0* (http://cisco.com/en/US/docs/net_mgmt/network_registrar/7.0/user/guide/CNR70_UG_book.html)
- *Quick Start Guide for Cisco Network Registrar 7.0* (http://cisco.com/en/US/docs/net_mgmt/network_registrar/7.0/user/guide/CNR70_QS_book.html)
- *CLI Reference Guide for Cisco Network Registrar 7.0* (http://cisco.com/en/US/docs/net_mgmt/network_registrar/7.0/command/reference/CLIReferenceGuide1.pdf)

Notices

The following notices pertain to this software license.

OpenSSL/Open SSL Project

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/).

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com).

This product includes software written by Tim Hudson (tjh@cryptsoft.com).

License Issues

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit. See below for the actual license texts. Actually both licenses are BSD-style Open Source licenses. In case of any license issues related to OpenSSL please contact openssl-core@openssl.org.

OpenSSL License:

Copyright © 1998-2007 The OpenSSL Project. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions, and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)".
4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.
5. Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project.
6. Redistributions of any form whatsoever must retain the following acknowledgment:

   "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)".

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT "AS IS"' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Original SSLeay License:

Copyright © 1995-1998 Eric Young (eay@cryptsoft.com). All rights reserved.

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com).

The implementation was written so as to conform with Netscapes SSL.

This library is free for commercial and non-commercial use as long as the following conditions are adhered to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgement:

   "This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)".

   The word 'cryptographic' can be left out if the routines from the library being used are not cryptography-related.

4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement: "This product includes software written by Tim Hudson (tjh@cryptsoft.com)".

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The license and distribution terms for any publicly available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution license [including the GNU Public License].

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 a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.
